SUBMISSION TO THE

AUSTRALIAN LAW REFORM COMMISSION

REVIEW OF PRIVACY IN RESPONSE TO

ISSUES PAPER 31

FROM

PROFESSOR MARGARET OTLOWSKI

ASSOCIATE PROFESSOR DIANNE NICOL

PROFESSOR DON CHALMERS

ON BEHALF OF THE

CENTRE FOR LAW AND GENETICS

JANUARY 2007

Introductory Comments: explanation of approach to our submission

This submission on behalf of the Centre for Law and Genetics deals somewhat selectively with the issues raised in this *Issues Paper*. In particular, it seeks to respond to those questions in the *Issues Paper* which concern the privacy regulation of health information.

We submit that question 4-36 is fundamental in raising the issue of whether the Privacy Principles should be prescriptive or should provide high-level guidance only. Overall, we submit that the co-regulatory model should continue, with the Privacy principles providing high level guidance supported by industry codes. However, we submit that the process for developing, approving and implementing industry codes must be improved and the Office of the Privacy Commissioner (OPC) must be given greater authority to ensure that this side of the co-regulatory model actually works. In particular, the enforcement provisions of the legislation need strengthening: this is a prerequisite to the effective development of the co-regulatory system.

This, in turn picks up on some of the fundamental issues raised in the *Issues Paper* about the most effective means of protecting the privacy of health information: in particular, whether it should be dealt with as part of the Commonwealth privacy legislation, or whether it should be the subject of separate regulation. We submit, with particular reference to health information, that this is best protected through a national code and enhanced and improved powers in the OPC.

The submission also addresses a few other areas where we have the knowledge and expertise to provide comment. Where we have no comment on specific questions, we have simply deleted the question from our submission.

1. Introduction to the Inquiry

1–1 Should the *Privacy Act* be amended to provide direct protection to groups such as: (a) Indigenous or other ethnic groups; or (b) commercial entities? If so, which groups or commercial entities should be covered by the Act?

In our view there is good justification for expanding the *Privacy Act* to provide direct protection of groups of natural persons, particularly indigenous and other ethnic groups. This is consistent with the emerging recognition of groups, rather than the traditional recognition of individual rights. There are some examples of recognition of groups in law through class actions, in research ethics (Chapter 8, Collectivities in the current National Statement on Ethical Conduct in Research Involving Humans) and in international law instruments. The underlying ethical rationale for privacy protection, based as it is in notions of human dignity and autonomy, clearly supports this expansion. Common law and equitable principles as they presently stand are simply too vague and uncertain. There should be appropriate laws in place to protect the privacy of information that may have great cultural and spiritual significance to

groups of indigenous and other ethnic peoples. We see no justification for challenging the prevailing view of the underlying rationale for privacy protection. Moreover, we see no particular justification for amending the *Privacy Act* to include direct protection for commercial entities.

1–2 Should a cause of action for breach of privacy be recognised by the courts or the legislature in Australia? If so, and if legislation is preferred, what should be the recognised elements of the cause of action, and the defences? Where should the cause of action be located? For example, should the cause of action be located in state and territory legislation or federal legislation? If it should be located in federal legislation, should it be in the *Privacy Act* or elsewhere?

It is most surprising that the Australian courts have yet to develop common law or equitable principles for breach of privacy in Australia. Australia is becoming increasingly out of step with other common law jurisdictions in this regard. It may well be that the courts would be amenable to such a development, should the right case come before them. In the absence of common law or equitable protection, there is good justification for the development of legislation to fill the void. Such legislation could provide protection against harassment-type invasion of privacy (as illustrated in the *Grosse* case) and against disclosure-type privacy (as illustrated in the *Lenah Game Meats* case – albeit a case which was destined to fail because the plaintiff was not a natural person). Case law in other jurisdictions provides guidance as to the suitable elements for the causes of action and defences. Should such legislation be developed, it is critically important that it should be consistent across Australia, either as uniform state and territory legislation through agreement between the relevant Ministers or as federal legislation. We do note, however, that whilst such legislation is desirable, it is probably unlikely that legislatures would be willing to take such a major step.

2. Overview of Privacy Regulation in Australia

2–1 Is national consistency in the regulation of personal information important? If so, what are the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia?

It is our view that national consistency in the regulation of personal information is indeed important and should be one of the objectives of any privacy reforms for Australia. National consistency will also enable the development of consistency with emerging international privacy standards (for example, as the *Issues Paper* mentions, the NPPs were influenced by the EU Directive on Data Protection). National consistency is also an essential response to the nationalising and internationalising of business, credit, banking and health services. Significantly, this has been the unanimous view of the Senate Committee inquiry into privacy and the Review undertaken by the OPC. This does not necessarily preclude, however, special privacy regulation applying to some areas (for example, health) – provided that this is also applied in a nationally consistent way. In other words, we believe the goal of national consistency can and should be aimed for but this does not limit the opportunity to deal with some areas in the most effective way possible. Uniform legislation should not be pursued at the expense of optimal legislation.

On the issue of the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia we note that there are a number of options put forward ranging from national legislation to non-binding codes. Our preference would be for comprehensive national legislation or some form of complementary scheme provided that consistency could be assured. Above all, there needs to be a strong, effective and enforceable regime in place.

3. The *Privacy Act 1988* (Cth)

3–1 Is the structure of the *Privacy Act* logical? Does the *Privacy Act* need to be redrafted to achieve a greater degree of simplicity and clarity?

We agree with the view expressed in the *Issues Paper* that the Commonwealth *Privacy Act* has become unduly complex and difficult to work with. In large part, this is due to the significant amendments that have been made to the legislation since it was first introduced in 1988. We would strongly support the redrafting of the legislation to achieve a greater degree of simplicity and clarity. Nevertheless, the original flow from collection through to release arose from the OECD Guidelines and this remains a defensible template. However, some revisions are required to bring consistency between the IPPs and NPPs and also some simplification, eg bringing together use and disclosure.

3–2 Insofar as the *Privacy Act* is primarily concerned with data protection, is the name of the *Privacy Act* accurate and appropriate?

We would support changing the name of the legislation to make its coverage more explicit: based on the models available in New South Wales and Tasmania, it could for example, be renamed the 'Privacy and Personal Information Protection Act' which would more clearly reflect the content and objectives of the legislation and help avoid public misapprehension as to its scope.

3–3 Is there some benefit in amending the *Privacy Act* to include the objects of the legislation? If so, what should be included in the objects clause?

We are of the view that there are good reasons for including in the *Privacy Act* the objects of the legislation. We have stated that we support the idea of the Privacy Principles being for guidance only, supported by industry codes. Clarity about this central objective of the legislation is vital. Furthermore, specifying the other key objects within the legislation is crucial in code development. It addition, specifying objects of the legislation, together with an appropriate change of name further to submission 3-2 above, would also assist in raising public awareness about the scope and operation of the legislation. As noted in the *Issues Paper*, inclusion of objects can also be of valuable assistance to courts and others charged with the interpretation of the legislation.

3–4 Are the definitions in the *Privacy Act* adequate and appropriate? For example, are the definitions of 'personal information' and 'sensitive information' in the *Privacy Act* adequate and appropriate?

We note the discrepancies in the coverage of the legislation (for example, recognition of the need for higher level of protection of 'sensitive information' for the purpose of the NPPs but not the IPPs). We are of the view that there needs to greater consistency in the coverage of the legislation, breaking down the division between the two categories of privacy principles for private/public. However, as outlined below, we are also of the view that privacy of health information is sufficiently unique and complex to justify separating this out from other forms of 'sensitive information' to ensure optimal regulation of this area.

We note that there are problems with other definitions in the *Privacy Act* as well. For example, the private sector amendments provide, in s6C, guidance about what is an organisation. It includes:

- an individual;
- a body corporate;
- a partnership;
- any other unincorporated association; or
- a trust

that is not a small business operator…

Other provisions in the Act impose privacy obligations generally on organisations, and therefore the question of who is an organisation is an important one. The difficulty is that s6C is unclear in its ambit, particularly with respect to the issue of which individuals are organisations for the purposes of the Act. In our view, the term is probably limited to individuals who are acting in the course of trade and commerce (this would bring the term within the limits of Commonwealth competence under the Constitution). However, the term is open to other interpretations and the explanatory memorandum provides no further guidance. This issue becomes particularly important in respect of the privacy obligations imposed on medical practitioners, for example.

3–5 Should the definition of 'personal information' in the *Privacy Act* be amended to include personal information of the deceased?

We are of the view that there are good justifications for extending the definition of personal information in the *Privacy Act* to include personal information of deceased persons. The justification for doing so is strongest with regard to aboriginal communities, who have religious and spiritual concerns about representations of deceased persons. Secondly, the justification extends to health information (for example, genetic information which has implications for relatives, or sensitive health information such as HIV/AIDS status) and we note the initiatives underway for implementing this. It could be argued, however, that a wider approach is appropriate extending protection to all personal information of a deceased person, as has been done under the *Personal Information Protection Act 2004* (Tas).

4. Examination of the Privacy Principles

By way of preliminary observation we note that the discussion in Chapter 4 highlights the unnecessary complexity of having different parallel regimes for the public and private sector (IPPs alongside the NPPs). As outlined below, we are of the view that

there is scope to rationalise these principles in a more unified form applicable across public and private sectors, but with provision for specialised treatment of health information.

4–1 Are the obligations imposed on organisations at the time of collection of personal information adequate and appropriate? For example, should an organisation also be required to make an individual aware of (a) the types of people, bodies or agencies to whom the organisation usually discloses information of that kind; (b) the various avenues of complaint available; and (c) the source of the information, where it has not been collected directly from the individual?

We are of the view that there are some gaps in the obligations imposed on organisations at the time of collection of personal information which ought to be addressed. In particular, we believe that organisations should be required to make an individual aware of:

(a) the types of people, bodies or agencies to whom the organisation usually discloses information of that kind;

(b) the various avenues of complaint available. (This is important to help overcome the numerous barriers that exist to effective redress of grievances, including lack of knowledge of available avenues of complaint.)

and

(c) the source of the information, where it has not been collected directly from the individual as this may be very material to the individual concerned.

4–2 Should NPP 1 be amended to clarify that there may be circumstances in which it is reasonable for organisations to take no steps to ensure that an individual is aware of specified matters relating to the collection of personal information?

Yes, we are of the view that this is appropriate in the interests of transparency.

4–3 Are the obligations imposed on agencies at the time of collection of personal information adequate and appropriate? In particular, should agencies also be subject to a general requirement that where reasonable and practicable, they should collect information about an individual only from the individual concerned? Should agencies also be required to notify an individual of his or her rights of access to the information, the consequences of not providing the information, the various avenues of complaint available, and the source of the information, where it has not been collected directly from the individual?

With regard to the question whether agencies should be subject to a general requirement that where reasonable and practicable, they should collect information about an individual only from the individual concerned, we submit that, in the interests of consistency, the approach taken *vis a vis* organisations on this issue should also apply to the collection of personal information by agencies. Further, we are of the

view that agencies should be required to notify an individual of his or her rights of access to the information, the consequences of not providing the information, the various avenues of complaint available, and the source of the information, where it has not been collected directly from the individual.

4–4 Should any obligations attach to an agency or organisation which receives unsolicited personal information that it intends to include in a record or generally available publication? If so, what obligations should be imposed?

The distinction between solicited and unsolicited personal information has historical relevance to surveys, paper documentation and paper-based record keeping. This distinction should not be maintained in a modern computer-data driven environment. The general duties regarding privacy should not be based on outdated distinctions that may encourage schemes of avoidance. We are of the view that if an agency or organisation proposes to include in a record or generally available publication, unsolicited personal information that it has received, it should be subject to the overarching privacy obligations with respect to that information. These obligations should not depend on whether the information was solicited or 'unsolicited personal information'. Irrespective of whether or not an agency or organisation controls the initial receipt of this information, if the agency or organisation proposes to include that information in a record there does not appear to be any valid justification for exempting such information from the usual regulatory requirements.

4–5 Should the obligations imposed on an organisation or agency at or soon after collection apply irrespective of the source of personal information?

We support the view promoted by the OPC that the obligations of organisations (and, we would submit, agencies) should apply to the collection of *all* information, irrespective of the source of that information, including information collected from publicly available sources. Significantly, we note from the *Issues Paper* that the Information Sheet developed by the OPC with regard to the interpretation of NPP 1.5 to this effect has gained widespread acceptance.

4–6 Is it desirable for the IPPs to deal separately with the principles relating to the use and disclosure of personal information or should use and disclosure be provided for in one principle?

We agree with the view that it would be more practical and effective for the issues concerning use and disclosure to be dealt with together in one principle, especially given that 'disclosure' can be characterised as a form of use. Significantly, this is in accordance with the OECD Guidelines and with the approach under the NPPs (Principle 2).

4–7 Are the circumstances in which agencies and organisations are permitted to use and disclose personal information under IPPs 10 and 11, and NPP 2, adequate and appropriate? In particular, should agencies and organisations be permitted expressly to disclose personal information: (a) to assist in the investigation of missing persons; (b) where there is a reasonable belief that disclosure is necessary to prevent a serious and/or imminent threat to an individual's safety or welfare, or a serious threat to public health, public safety

or public welfare; and (c) in times of emergency? What mechanism should be adopted to establish the existence of an emergency?

We are of the view that each of the following circumstances justify the creation of an exception to the normal rules regulating the use and disclosure of personal information as the public interest in disclosure outweighs the private (and public) interest in the protection of this information:

(a) to assist in the investigation of missing persons;

(b) where there is a reasonable belief that disclosure is necessary to prevent a serious and/or imminent threat to an individual's safety or welfare, or a serious threat to public health, public safety or public welfare;

and (c) in times of emergency.

It is important, however, that the exceptions are drafted no wider than necessary.

With regard to the most appropriate mechanism to adopted to establish the existence of an emergency, We are of the view that the mechanism proposed by the OPC as set out in para 4.80 of the *Issues Paper*, would appear reasonable.

4–8 Are the criteria in NPP 2.1(a) for using personal sensitive and non-sensitive information for a secondary purpose adequate and appropriate? For example, is it necessary or desirable that there also be a 'direct' relationship between the secondary and primary purpose of collection before non-sensitive personal information can be used or disclosed for a secondary purpose?

It would seem desirable to require that there be a 'direct' relationship between the secondary and primary purpose of collection before non-sensitive personal information can be used or disclosed for a secondary purpose. We would accordingly support an amendment to NPP 2.1(a) so that this is stipulated as a requirement in respect of *all* personal information, not just for 'sensitive information'.

4–9 Is the scope of IPP 10(e) (which allows agencies to use personal information for a purpose other than the particular purpose of collection, if the purpose for which the information is used is directly related to the purpose of collection) adequate and appropriate? For example, should there be an additional requirement that the individual concerned would reasonably expect an agency to use the information for that other purpose?

Yes, imposition of an additional requirement on the power of agencies to use personal information for a purpose other than, but directly related to, the purpose of collection, namely, that the individual concerned would reasonably expect an agency to use the information for that other purpose would appear to be reasonable.

4–10 In what circumstances should agencies or organisations be required to record their use or disclosure of personal information when it is used or disclosed for a purpose other than the primary purpose?

Generally, agencies and organisations should record any use or disclosure of personal information, whether it is for a primary or secondary purpose. Such a record can be easily generated if the data is electronic. This tracking can be audited and provides an overarching obligation of accountability for those using data (see our response to Question 4-35.

4–12 Is it appropriate that NPP 2 allows for personal non-sensitive information to be used for the secondary purpose of direct marketing? If so, are the criteria that an organisation needs to satisfy in order to use personal information for direct marketing purposes adequate and appropriate?

Ongoing use of personal non-sensitive information for direct marketing may well be appropriate in some circumstances. However, we believe that the current opt-out requirements are inadequate. At the very least, a time frame for compliance should be specified, but in our view this does not go far enough. Given the pervasiveness of direct marketing we suggest that opting-in requirements should be the norm. We note that the Internet Industry Association draft privacy code prefers the opt-in model. If it were the case that privacy codes imposing standards higher than the NPPs (including opting-in provisions relating to direct marketing, for example) were prevalent across many industry sectors, we may be persuaded that the opting-out requirements in NPP2 would suffice. However, this is simply not the case. As noted in the *Issues Paper,* only four codes have been approved to date. In general, privacy codes largely reiterate the NPPs, rather than imposing significantly higher standards. We suggest that NPP2 should specify that opting-in is required for use of personal information for direct marketing purposes, subject to certain exceptions. For example, it may be desirable to exclude charitable organisations from this requirement. The list of exceptions in the *Spam Act* could provide guidance in this regard. Other legislation could specify a lower standard in certain circumstances. In summary, we are suggesting that the privacy principles should do more than simply set 'a minimal standard only' (*Issues Paper* at 153).

4–13 Should use and disclosure of personal information be allowed for research that does not involve health information—for example social science research? If so, in what circumstances or upon what conditions might this be appropriate?

We are of the view that there should be provision for the use of personal information for research other than health research which may also be of benefit to the community such as social science research. Indeed, if research involving health information is permitted, which is a category of sensitive information, there is a strong case to argue that other forms of personal information that do not fall into the sensitive category of health information should also available for legitimate research use. Useful guidance on the appropriate circumstances or conditions under which personal information should be able to be used and disclosed for this purpose can gained from the privacy legislation that has been introduced in Canada as well as that in a number of Australian states. Drawing on these models, it could, for example, be specified that personal information necessary for research or for the compilation or analysis of statistics, in the public interest, in a manner which does not identify any particular individual may be used if it is impracticable for the organisation to obtain individual consent before the use or disclosure, and in the case of disclosure the organisation

making the disclosure reasonably believes that the recipient of the information will not disclose the information.

4–14 Is the scope of the data quality principle in NPP 3 (which requires an organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date) adequate and appropriate? For example, should the principle expressly apply to information that an organisation controls?

In the interests of greater consistency between the NPPs and the IPPs, the scope of NPP 3 should be extended to apply to personal information that an organisation controls but which is not necessarily in the direct possession of the organisation. In addition, it would be desirable to include a further requirement as part of the data quality principle, following the OECD model, that the information be relevant at the time of collection.

4–15 Is there a need to amend NPP 3 to clarify the extent of the obligations of an organisation under the data quality principle or is this best dealt with by way of guidance issued by the Office of the Privacy Commissioner?

It may be preferable to follow the approach taken under the Canadian privacy legislation and OECD Guidelines to explicitly spell out that the obligation on organisations to maintain data quality is a qualified one. This may be more effective in helping to combat what appear to be defensive practices by some organisations rather than relying on further guidance from the OPC.

4–16 Should agencies be subject to a stand-alone data quality principle that extends to the collection, use and disclosure of personal information?

Yes, in the interests of consistency, but this should also be qualified as per submission in para 4-15 above.

4–17 Is the scope of NPP 4 relating to the obligations of an organisation to secure data adequate and appropriate? For example, should NPP 4 be amended to impose an obligation on organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected?

Yes, in our view there should be an ongoing obligation on the part of the principal to ensure that the personal information they collect is protected, particularly when personal information is passed on to contractors that are not subject to the requirements of the *Privacy Act.*

4–18 Are there any circumstances in which agencies should be under an obligation to destroy or permanently de-identify personal information when it is no longer needed?

See comment below relating to 4-19.

4–19 Should the IPPs and the NPPs regulate the deletion of personal information by organisations and agencies? In what circumstances might this be

appropriate? Should an individual have the right to request that an agency or organisation destroy personal information that it holds or controls concerning the individual? If so, in what circumstances or upon what conditions should this be permitted?

We believe that the circumstances relating to obligations to destroy, permanently de-identify or delete personal information need clarifying. In particular, it should be made clear that the Guidelines relating to deletion of incorrect information are equally applicable to private sector organisations as well as federal government agencies. In addition, as a general principle, any deletion or permanent de-identification should eb recorded so that there is an audit trail that can be checked if required at some future date.

4–20 Is the scope of NPP 5 relating to openness adequate and appropriate? For example, is it necessary or desirable for organisations to be given greater legislative guidance about their obligations under the principle? Does the more prescriptive approach to the openness principle in IPP 5 provide a suitable model?

As a general principle, the privacy legislation should establish overarching principles, in this case, of openness. The codes should then operationalise this principle to specific contexts. Generally we believe that it is beyond the legislation to spell out giudance in particular contexts. However, as we say elsewhere, these codes must be strengthened and improved.

4–22 Is there a need to clarify the relationship between the obligation of an organisation under NPP 1.3 (which imposes an obligation on organisations to take reasonable steps to ensure that an individual is aware of specified matters at or before the time of collection) and NPP 5.1 (which imposes an obligation on organisations to set out in a document clearly expressed policies on its management of personal information)? If so, how is this best achieved?

Yes, there needs to be greater clarification between NPP1.3 and NPP5.1. This is an example of the need to improve the overall relationship between the Act and the codes. We submit that NPP1.3 is an example of an overarching principle that should be in the legislation, whereas NPP5.1 is operational and is required to be included in a given code. We submit that this distinction between principles and operational matters is crucial, and that NPP5.1 would perhaps be better placed in a schedule of basic required content for codes.

4–23 Are the circumstances in which organisations can deny an individual access to his or her personal information under NPP 6 adequate and appropriate? If the circumstances are inadequate, should this be addressed by legislative amendment to the principle or by guidance issued by the Office of the Privacy Commissioner?

We submit that circumstances should remain in the legislation, consistent with FOI legislation, and not issued as geenral guidance from the OPC.

4–25 Should the *Privacy Act* be amended to impose an obligation on both agencies and organisations to notify third parties, where practicable, that they have received inaccurate information and to pass on any corrected information? Should an obligation to notify third parties apply where agencies or organisations have refused to make a correction?

We submit that there should be an obligation on agencies and organisations to notify third parties, including where they have refused to make a correction.

4–26 Is there a need for a separate privacy principle regulating the adoption, collection, use and disclosure of identifiers by organisations? Should NPP 7, the principle regulating identifiers, be redrafted to deal more generally with the issue of data-matching?

We are strongly of the view that privacy principles should extend to data matching. Modern technology enables sophisticated data matching and it may be timely for there to be a separate principle on this issue.

4–28 Should the *Privacy Act* be amended to regulate the assignment, adoption, collection, use and disclosure of identifiers by agencies?

We submit that the *Privacy Act* needs to be amended to regulate these matters. The reason for this is to enable the OPC to audit the activities of these agencies and, if necessary, to conduct investigations into them. However, we note that this may not be possible at the moment.

4–29 Should NPP 8, the anonymity principle, be redrafted to impose expressly an obligation on organisations to give an individual the option of remaining anonymous when entering into transactions with those organisations?

4–30 Is it appropriate or desirable for agencies to be subject to an anonymity principle? In what circumstances, if any, might this be appropriate?

We support the general principle of anonymity. However, we have genuine reservations about whether anonymity is realistic in the modern computer age.

4–31 Should the transfer of personal information offshore by agencies be regulated by privacy principles?

We submit that transfer of information offshore by agencies, just as much as by organisations, should be regulated by privacy principles. This has already been recognised in the NPPs as part of our international obligations, particularly with regard to the EU. It should be extended to the IPPs.

4–32 Should federal privacy principles allow agencies and organisations to collect non-health related sensitive information for other purposes, including research and statistical purposes? If so, in what circumstances should this be permitted?

A case can certainly be made for public bodies to be allowed to collect non-health related sensitive information for other purposes, including research and statistical purposes following the model adopted in Victoria and the Northern Territory. Whilst the case for *public* bodies to do so is stronger, such an exception might also be extended to private organisations in appropriate circumstances, subject to reasonable conditions and safeguards including some form of public interest test.

4–33 Should federal privacy principles establish a separate regime for the public and private sectors regulating sensitive information in all aspects of the information cycle, including collection, use, disclosure, storage, access, retention and disposal? If so, what should that regime include?

Given that 'sensitive information' is recognised under the legislation, it would be logical for there to be greater consistency, ensuring that the higher level of protection applies in respect of both the public and private sectors, and to all aspects of the information life cycle, including collection, use, disclosure, storage, access, retention and disposal.

4–34 Should the *Privacy Act* provide a uniform set of privacy principles that are to apply to both the public (currently covered by the IPPs) and private (currently covered by the NPPs) sectors? If so, what model should be used? Are there any particular principles or exceptions to principles that should apply only to either the public or private sector?

We are of the view that having two sets of parallel principles which may both apply to an organisation or agency's operation is unduly complex and confusing and that it would be preferable for there to be a single set of privacy principles regulating both sectors. This would be in line with the approach adopted by the OECD Guidelines. As to which model, the NPPs are of more recent origin and have been influenced by international requirements. These principles have also been influential in the development of principles under the Privacy Acts in Victoria, Tasmania and the Northern Territory. Moreover, the NPPs were developed for the private sector taking account of compliance capacity: to use these as the framework for developing principles for both the public and private sector would obviously entail change for the public sector but would keep to a minimum the compliance burden and costs of such a change for Australia as a whole. We acknowledge that there may be a need to modify the application of the unified principles for one sector or another. This needs to be carefully worked through but as a matter of principle, we are strongly in support of a more homogenous and uniform approach to privacy regulation in Australia.

4–35 Apart from the principles contained in the IPPs and NPPs, are there any other principles to which agencies and organisations should be subject? For example, should the IPPs and NPPs include expressly: an 'accountability' principle; a 'prevention of harm' principle; a 'consent' principle; or a requirement that agencies and organisations notify persons whose personal information has been, or is reasonably believed to have been, accessed without authorisation? If so, what should be the content of these principles?

Review of the position in overseas jurisdictions reveals some interesting initiatives and approaches which are definitely worth considering in Australia, in particular, we

are attracted to the inclusion of certain overriding principles of 'accountability' and 'prevention of harm' and see an opportunity here to send a very positive message to members of the public about the aims of privacy regulation in Australia. These overriding principles are consistent with the approach of the *Privacy Act* providing general guidance and details being included in industry Codes of Practice. In addition to 'accountability' and 'prevention of harm', the principles of 'transparency' and 'notification' could be included. With respect to the latter we would support a requirement that agencies or organisations should be obliged as a general principle to 'notify' persons whose personal information has been or is reasonably believed to have been accessed without authorisation.

4–36 Should federal privacy principles be prescriptive or should they provide high-level guidance only? Should they aim for a minimum or maximum level of protection of personal information or aim to adopt a best practice approach?

This is one of the key central issues raised in the document. We are of the view that the privacy principles already have a history of providing guidance. This high level guidance approach is supplemented by Codes of Practice. Provided the OPC is given additional powers to encourage, or in some cases, impose these Codes, the high level guidance approach is preferred. We acknowledge that there are pros and cons with either a prescriptive approach or one which provides high level principles. We are of the view that developing a midway approach between these two positions aiming at a 'best practice approach' would be most appropriate and would mitigate the problems arising at either extreme.

5. Exemptions from the *Privacy Act 1988* (Cth)

Whilst we do not propose to make detailed comments on this area of exemptions, there are a few general comments and observations that we would like to make. We share the concerns raised in the *Issues Paper* regarding the substantial number of exemptions under the legislation. This growth of exemptions, if unchecked, has the potential to undermine the operation of the principles contained in the legislation and compromise the privacy rights of individuals. We would endorse the approach of the OECD Guideline which state that 'exceptions to the privacy principles should be as few as possible'. We also share concerns about the complexity of the exemption provisions and the difficulty of finding them as they are scattered throughout the Act. We support a thoroughgoing reevaluation of the existing exemptions to establish which exemptions are justifiable to retain and once that is ascertained, for a reconfiguration of the legislation so that exemptions which are permitted are more clearly visible within the legislation.

5–1 Is it appropriate for certain entities to be exempt, either completely or partially, from the operation of the *Privacy Act*? If so, where should the exemptions be located?

Generally, we consider that the exemptions should be limited and justified. Generally, exemptions should only apply, as suggested by Question 5-2 to national security, defence and intelligence agencies.

5–2 Should the following defence and intelligence agencies be exempt, either completely or partially, from the *Privacy Act*:

- **Defence Imagery and Geospatial Organisation;**
- **Defence Intelligence Organisation;**
- **Defence Signals Directorate;**
- **Australian Security Intelligence Organisation;**
- **Australian Secret Intelligence Service; and**
- **Office of National Assessments?**

If so, what is the policy justification for the exemption? Are there any other defence and intelligence agencies that should be exempt, either completely or partially, from the *Privacy Act*?

It is not unreasonable that these agencies be exempt. The policy justification for this exemption rests on a claim of acting in the public interest. It may be appropriate to include this statement. This will establish a limitation for these agencies. Should any officer of any of these agencies seek out information for private purposes, they would be outside the public interest requirement. Secondly, it may be good practice to require that any access to personal information by these agencies should be recorded to enable access to be tracked and later audited.

5–3 Should the following agencies be exempt, either completely or partially, from the *Privacy Act*:

- **Australian Government ministers;**
- **federal courts;**
- **agencies specified in Schedule 1 to the *Freedom of Information Act 1982* (Cth)—namely, the Australian Industrial Relations Commission, the Australian Fair Pay Commission, the Industrial Registrar and Deputy Industrial Registrars;**
- **Australian Crime Commission;**
- **royal commissions;**
- **Integrity Commissioner;**
- **agencies specified in Schedule 2 Part I Division 1 of the *Freedom of Information Act 1982* (Cth) other than the intelligence agencies, the Australian Government Solicitor and the Australian Industry Development Corporation; and**
- **agencies specified in Schedule 2 Part II Division 1 of the *Freedom of Information Act 1982* (Cth)?**

If so, what is the policy justification for the exemption? Are there any other agencies that should be exempt, either completely or partially, from the *Privacy Act*?

In our view it is entirely appropriate for courts to be partially exempted from the provisions of the *Privacy Act* because of the overriding principle of open justice. The present provisions largely reflect an appropriate balance between the principle of open justice and the privacy of personal information. We are of the view that it is appropriate to retain the partial exemption for judicial records and to leave it to other

legislation to impose higher order restrictions on access to court documents and hearings. However, we do acknowledge that the lack of consistency nationally is problematic. Nevertheless, we suggest that this matter should be dealt with in separate legislation, for example an *Access to Court Records Act* rather than adding further complexities to the already over-burdened *Privacy Act.*

We also note that a number of these other agencies are subject to specific legislation. For example, Royal Commissions are governed by State and Territory legislation that includes specific provisions about witnesses, evidence and access to information.

5–4 Should state and territory authorities be exempt from the privacy principles in the *Privacy Act*?

This question raises the more general issue of the need for consistency between Australian and State and Territory legislation. Under a unified system, particular exemptions for State and Territory authorities could be included in the corresponding State and Territory privacy legislation. The Gene Technology Regulatory Scheme under the *Gene Technology Act* 2000 (Cth) and the corresponding State and Territory legislation provides a good example.

5–6 Should the small business exemption remain? If so: (a) what should be its extent; and (b) should an opt-in procedure continue to be available?

In our view there is no longer any justification to retain the small business exemption. Justifications for the small business exemption (particularly relating to the cost of compliance) may well have been sound in 2000, when the private sector amendments were passed. However, it is hoped that the NPPs reflect best practice with regard to the protection of personal information, and all organisations collecting personal information should be following best practice. All organisations should by now have had sufficient time to adapt their practices to meet NPP standards and it is difficult to see how this exemption can be retained.

The NPPs should be designed to provide an appropriate balance between an individual's right to privacy and the free flow of information. As such, arguments that a large number of organisations in the private sector should be exempted based on business efficacy are, in our view, no longer sustainable.

5–7 Should registered political parties be exempt from the operation of the privacy principles in the *Privacy Act?*

We are strongly of the view that there should be no exemption for political parties. Political parties should act in the public interest and should not be allowed to breach public privacy standards for political ends. There have been recent concerns that the staff of elected parliamentarians sometimes go beyond service to their electorate and involve themselves in overtly political promotion and lobbying.

5–9 Should the employee records exemption remain? If so: (a) what should be the scope of the exemption; and (b) should it be located in the *Privacy Act*, workplace relations legislation or elsewhere?

We are concerned about the lack of adequate privacy protection for private sector employees under the federal workplace relations regime. This is completely out of step with the approach applying to employees in the public sector both under the IPPs and state privacy legislation. Notably, there is no general exemption for employee records under the OECD Guidelines. Not surprisingly, this has been one of the sticking points in Australia gaining 'adequacy status' under the EU Directive. Information held by employers about the employees may be very sensitive, including health and financial information and there is real potential for individuals to be harmed if this information is inappropriately used or disclosed. It is also noteworthy that a significant number (12%) of the complaints closed by the OPC as falling outside its jurisdiction concern the employee records exemption. We would argue that the employee records exemption in the *Privacy Act* should be repealed so that all employee records are subject to the protection of the NPPs.

5–10 Should acts and practices of media organisations in the course of journalism be exempt from the operation of the *Privacy Act*? If so: (a) what should be the scope of the exemption; and (b) does s 7B(4) of the *Privacy Act* strike an appropriate balance between the free flow of information to the public and the protection of personal information?

Use of personal information by journalists raises particular concerns when the information is sensitive in nature. For example, in the Privacy Commissioner's review of the private sector provisions in the *Privacy Act, Getting in on the Act* in 2005, the Australian Medical Association (AMA) gave an example of privacy violation caused by disclosure that a person was admitted to hospital for psychiatric care, which, according to the AMA, resulted in severe disruption the delivery of clinical care. Others in the area also expressed similar concerns.

Nevertheless, in our view there is still a need for some sort of exemption from the *Privacy Act* to ensure an appropriate balance between privacy and the free flow of information. We support the view that the exemption should be retained, but that there should be amendments to the Act to set appropriate limits on the exemption. For example, it may be appropriate to limit the exemption to use of non-sensitive personal information. Use of sensitive information could be governed by the NPPs, perhaps with the inclusion of a provision allowing publication where there is reasonable justification.

5–11 Should the terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' be defined in the *Privacy Act*? If so, how should they be defined? Are there other terms that would be more appropriate?

We support the view that these terms should be defined in the Act. We suggest that the definition of journalism that was included in the initial Privacy Amendment (Private Sector) Bill should be revisited. It is important that the privacy regime carefully balances the democratic interest and freedom of the press with the promotion of responsible journalism.

5–12 If the media exemption is retained, how should journalistic acts and practices be regulated?

Currently journalistic acts relating to use of personal information are inadequately regulated in some sectors, largely due to the lack of scrutiny of the adequacy of privacy standards and lack of enforceability of standards. There is a significant difference in the way that journalistic acts are regulated in the broadcasting, online and print media. The broadcasting medium has the most stringent regulation, as a result of the *Broadcasting Services Act 1992* (Cth). Once Codes of Practice are registered by the Australian Communications and Media Authority, the obligations contained therein become legally enforceable. Hence, self regulation of the use of personal information through Codes in the broadcasting medium may well be appropriate, provided that privacy standards have been vetted by the OPC. However, in the print medium, Press Council Principles have no legal force. In the online medium there is no equivalent self regulatory body. Whilst the Media Entertainment and Arts Alliance has a Code of Ethics and has some enforcement powers, there is no requirement for journalists to be members of the Alliance in order to rely on the media exemption.

The notion of public commitment to observe published standards needs to be clarified. We support the view that the OPC should determine whether standards are adequate and particularly whether they provide for sufficient sanctions against non-compliance. In situations where there are no standards, or where the standards are inadequate, the Privacy Commissioner should be given the power to direct that the Act must be complied with.

6. Powers of the Office of the Privacy Commissioner

We have already expressed support for the approach of high guidance principles supported by industry codes. To make this approach work, it is likely that the OPC will require additional powers to encourage and, in some cases, require the making of such Codes. Many of these questions will require consideration of the views of the current and past Privacy Commissioners to assess what additional powers are required. For this reason, many of the questions in this section are outside the practical knowledge of the CLG.

6–1 Is the legislative structure pertaining to the Office of the Privacy Commissioner established under the *Privacy Act* appropriately meeting the needs of the community?

Generally, we consider that the OPC has done a very good job within its resources in advancing privacy standards in this country.

6–6 Should the *Privacy Act* require a privacy impact assessment to be prepared for: (a) all proposed Commonwealth legislation; (b) other proposed projects or developments of agencies; or (c) other proposed projects or developments of organisations?

Australian legislation currently undergoes economic, human rights and environmental impact assessments. Arguably, privacy is a component of human rights and could form part of that assessment. We are of the view that some form of privacy impact assessment is desirable.

6–9 What powers should the Privacy Commissioner have to audit agencies and organisations?

This is a crucial issue. If the approach of general guidance principles and industry codes is to have any public credibility and practical effectiveness, the PC must have genuine powers to audit agencies and organisations. As the approach aims to develop a co-operative model, the OPC should have powers that require actions by the agency or organisation to address the problem *before* a mandatory audit. The power to carry out unannounced spot audits should be restricted to serious cases.

6–10 Should organisations and agencies be required to self-audit periodically to ensure and to demonstrate compliance with the *Privacy Act*?

To the best of our knowledge, some agencies and organisations are now taking privacy compliance very seriously, particularly in the public sector. It is likely that the inclusion of a general principle of periodic self-audit would not be an imposition. It is a principle that is consistent with best practice.

6–11 Should all the Privacy Commissioner's functions be consolidated in the *Privacy Act?*

This is the preferred approach.

6–12 Are the procedures under the *Privacy Act* for making and pursuing a complaint, including a representative complaint, appropriate? Are the Privacy Commissioner's powers to make preliminary inquiries and investigate complaints appropriate and effective?

From information in Annual Reports, inquiries and investigations are instituted, but the views of the OPC will be critical in deciding whether they are 'appropriate and effective'. If the development of industry codes is the preferred approach, the OPC must have appropriate and effective powers to ensure compliance.

6–18 Are the Privacy Commissioner's powers under the *Privacy Act* to make public interest determinations, including temporary public interest determinations, appropriate and administered effectively?

The PIDs are published by the OPC are not numerous and the temporary PIDs even less used. The lack of use of this power must be considered. However, we are aware of the more recent PID for the Insurance Council of Australia impacts on genetic testing, which has been generally very well received

6–20 Are the *Privacy Act* provisions for approving privacy codes appropriate and effective? Are privacy codes an appropriate method of regulating and complying with the Act? Why have privacy codes been so little used? Should the Privacy

Commissioner have the power, on his or her initiative, to develop and impose a binding code on organisations or agencies?

We believe that this is another crucial issue for the development of our preferred approach of general guidance principles supported by industry codes. The OPC must have power, where there has been a failure by the industry after reasonable notice, to develop and impose a binding code. Where such a code has been imposed, it may be reasonable there is an automatic review of the operation within a year or other reasonably short period. However, there must be such a power in the OPC, to ensure public confidence in the development of a national privacy regime.

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation

7–1 Does the multi-layered regulation of personal information create any difficulties? For example, does the multi-layered regulation of personal information:

(a) cause an unjustified compliance burden;

(b) create problems for organisations that operate in more than one Australian state or territory;

(c) complicate the implementation of programs and services at a national level;

(d) raise any issues in relation to the existence of multiple privacy regulators in particular industry sectors and across the states and territories; or

(e) act as a barrier to the sharing of information between public sector agencies and private sector organisations?

It seems self evident that the multi-layered, fragmented and inconsistent nature of privacy regulation in Australia is problematic. In particular, the division between regulation of public/private sectors (commented on above) and the growth of state privacy legislation due to the fact that the federal law does not cover the field are key factors which are presently detracting from a coherent national privacy scheme in Australia. The complexity that results, including the potential for overlap of regulation, such that a single piece of personal information may be subject to more that one legislative regime at the same time, is clearly contributing to the compliance burden and cost and impedes what may be appropriate sharing of information between sectors. Efforts to achieve rationalisation and greater uniformity are therefore needed.

7–2 Do any issues arise for organisations that provide contracted services involving personal information to Australian Government, state or territory agencies? For example:

(a) are privacy provisions in Australian Government, state or territory agency contracts contributing to inconsistency and fragmentation in privacy regulation;

(b) are the *Privacy Act* provisions relating to Commonwealth contractors appropriate and effective;

(c) do issues arise for Commonwealth contractors that are subject to the NPPs and the IPPs;

(d) do any issues arise for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies;

(e) is there a concern that organisations acting under a state or territory contract may not be required to adhere to the same privacy standards that are applicable to private sector organisations under the *Privacy Act*? If so, how should that concern be addressed?

We are of the view that a nationally consistent system is required. If there are inconsistencies created by different rules applying to contracted services between Australian and State and Territory agencies, this creates an economic efficiency objection beyond the need for legal consistency. Unnecessary legal cost to business should be reduced, consistent with Australian Government policies.

7–3 How should personal information held on residential tenancy databases be regulated? For example, should it be regulated under the *Privacy Act*, by a binding code, or in some other way?

Residential tenancy databases would be best regulated by a binding Code. It is inappropriate for the detailed operational rules of tenancy databases to be included in governing legislation. It is more appropriate that the *Privacy Act* establish the high level guidance with the details of specific industries included in binding Codes.

7–6 Does the interaction between the *Privacy Act* and other federal legislation that regulates the handling of personal information require clarification? In particular:

(a) does the overlap of the *Privacy Act* and *Freedom of Information Act 1982* (Cth) provisions relating to access and amendment of records give rise to any difficulties;

(b) should the *Privacy Act* provide for a process of consultation prior to granting access to information that includes personal information about a third party rather than rely on the process outlined in the *Freedom of Information Act 1982* (Cth);

(c) should the *Privacy Act* and the *Freedom of Information Act 1982* (Cth) be administered by the same body;

(d) should the *Privacy Act* apply to certain classes of records in the open access period for the purposes of the *Archives Act 1983* (Cth);

(e) should the exemption under the *Archives Act 1983* (Cth) relating to 'information relating to the personal affairs of any person' be amended to provide an exemption in relation to 'personal information' as defined in the *Privacy Act*;

(f) should the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth) be consolidated in one Act;

(g) should federal legislation relating to the handling of tax file numbers and data-matching be consolidated in one Act? If so, should they be consolidated in the *Privacy Act*;

(h) should data-matching programs that fall outside the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) be more formally regulated;

(i) is personal information collected pursuant to the *Census and Statistics Act 1905* (Cth) adequately protected;

(j) is it appropriate that the disclosure of a shareholder's personal details in a register of members, register of debenture holders or a register of option holders under the *Corporations Act* is a disclosure of personal information that is permitted for the purposes of NPP 2;

(k) does the *Commonwealth Electoral Act 1918* (Cth) provide adequate protection of personal information included on the electoral roll;

(l) does the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) adequately protect personal information?

We believe that serious consideration should be given to develop some simplification of the current overlap between the privacy and freedom of information legislation. Originally, the two Acts had distinct provenances, the former establishing duties for record collectors and keepers and the latter rights for citizens. Now, we believe there is a very good case for bringing the administration of these Acts together. On the other hand, the *Archives Act*, we believe, has a different and distinct function and should remain separate.

7–8 Are the provisions in Part VIII of the *Privacy Act* necessary? If so, are the provisions adequate and should they be contained in the *Privacy Act* or elsewhere?

This Part is rather odd and no doubt has a particular history. These confidentiality provisions do not appear to have been widely used. If this is confirmed by the OPC they should be deleted.

7–9 Do privacy rules, privacy codes and privacy guidelines developed under federal, state and territory legislation, or by organisations and industry groups, contribute to fragmentation and inconsistency in the regulation of personal information?

We are strongly of the view that the plethora of Australian State and Territory Rules, Codes and Guidelines, must be simplified not only to simplify the legal rules but to assist administrative and business efficiency.

8. Health Services and Research

8–1 Does the regulation of health information require a different and separate set of privacy principles to those used to regulate other sensitive personal information?

We are strongly of the view that there should be a separate set of privacy principles for the regulation of health information to those used to regulate other sensitive personal information. This is because of the highly sensitive and complex nature of health information, which includes different types of information within it, including the particularly sensitive area of genetic information which is not only very personal information, but also has a shared, familial dimension. Enacting a separate set of privacy principles dedicated to health information would allow the privacy standards to accommodate the particular characteristics and the sensitive nature of health information in general. Further, it would allow scope for developing particular provisions within that set of principles recognising the special nature of certain types of health information such as genetic information, and related issues such as the 'right not the know' and disclosure of genetic information to blood relatives. It would, however, avoid assumptions about genetic information being uniquely sensitive (and related arguments about 'genetic exceptionalism') and would allow special provision to be made for the protection of other particularly sensitive health information. Notably, the inclusion of health information as part of the major amendments to the federal privacy legislation in 2000 was one of the most contentious aspects of that legislation so this has been a troublesome approach from the outset. Added to the difficulty has been the fragmented nature of the coverage with 'health information' given special recognition under the NPPs but not the IPPs and the emergence of state and territory legislation also seeking to regulate this area. Not surprisingly, the goal of harmonisation and national consistency for health information privacy has now been on the agenda for some years and was strongly endorsed also by the ALRC/AHEC *Essentially Yours* Report (2003).

8–2 Should s 3 of the *Privacy Act* be amended to state that the Act is intended to regulate the handling of health information in the private sector to the exclusion of state and territory legislation?

We can see the advantage of a clear statement within the federal *Privacy Act* that it intends to cover the field in this area, particularly in the light of the proliferation of state and territory legislation in this area and the resulting fragmentation of coverage. This would at least address the complexities arising from overlapping coverage of legislation (both federal and state or territory) and would ensure that as far as possible, private sector health service providers and health and medical researchers would only be required to comply with one regime. In our view, however, more far-reaching reforms are required to achieve the desired national consistency in regulation of health information. Such an amendment would not, for example, address the inconsistency in coverage with regard to health information between public and private sectors in the federal *Privacy Act.*

8–3 Is the draft *National Health Privacy Code* an effective way to achieve a nationally consistent and appropriate regime for the regulation of health information? If so, what is the most effective model for implementing the draft *National Health Privacy Code?* If not, what other model should be adopted to achieve a nationally consistent and appropriate regime for the regulation of health information?

We are of the view that the draft *National Health Privacy Code* is an effective way to achieve a nationally consistent and appropriate regime for the regulation of health information in Australia, subject to some modification. Two of us have already provided a submission to the AHMAC relating to the draft Code, a copy of which is attached in Appendix A. That submission focused primarily on the need to take into account the special issues relating to genetic information.

So far as the most effective model for implementing the draft *National Health Privacy Code* is concerned, we would support national health privacy legislation as the preferred option to maximize visibility, and ensure ongoing uniformity of coverage of this area which in our view would be much harder to achieve under a co-operative scheme involving applied or mirror legislation.

8–4 If the draft *National Health Privacy Code* is not implemented nationally, should the Australian Government adopt the Code as a schedule to the *Privacy Act*?

If the preferred option of legislative implementation of the *National Health Privacy Code* proves unobtainable due to lack of co-operation from all jurisdictions, this proposal of adopting the Code as a schedule to the *Privacy Act* may be appropriate as a fall back position however, it is not entirely clear what status or force this would have.

8–5 Do electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or the draft *National Health Privacy Code*?

The development of the Health*Connect* system, to the best of our knowledge has tried to develop consistency with the *Privacy Act* and the National Health Privacy Code. We do not believe that additional privacy rules should be developed. Health information systems should comply with the general guidance principles and the details should be included in the Draft Code. No doubt other information can be gathered from those involved in setting up these electronic health information systems.

8–6 The *National Health Act 1953* (Cth) requires the Privacy Commissioner to issue guidelines in relation to the handling of personal information collected in connection with claims under the Medicare Benefits Program and the Pharmaceutical Benefits Program. Is this an appropriate and effective role for the Privacy Commissioner?

The views of the OPC should be carefully considered in respect of this issue.

8–7 Are the definitions of: (a) 'health information'; and (b) 'health service' in the draft *National Health Privacy Code* appropriate and effective? Should the *Privacy Act* be amended to adopt these definitions?

The definition of health information in the draft *National Health Privacy Code* is a fuller, more encompassing definition and is in keeping with the more contemporary definitions of health information in state and territory legislation (NSW *Health Records and Information Privacy Act* (2002), Victorian *Health Records Act* (2001), and the Northern Territory *Information Act* (2002)). We would be in support of amending the *Privacy Act* to adopt this definition. Similarly, the definition of 'health service' in the draft *National Health Privacy Code* is more explicit and inclusive in its coverage and also would appear to be appropriate and effective and suitable for adoption in the *Privacy Act.*

8–8 Should the *Privacy Act* be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act?

Yes, in the interests of consistency and ensuring as uniform coverage as possible, we are of the view that the *Privacy Act* be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act.

8–9 Is guidance by the Office of the Privacy Commissioner to clarify that organisations can disclose health information for the management, funding and monitoring of a health service an appropriate and effective response to concerns in this area? If not, what is an appropriate and effective response?

It may be preferable to address this issue through amendment of the *Privacy Act*; this would in our view, offer a clearer and more certain solution to the current lack of clarity around this issue.

8–10 Is there evidence that the regulation of personal health information impedes the provision of appropriate health services to individuals? If so, what changes are necessary to facilitate the provision of appropriate health services?

Whilst we are not in a position to advise as to whether there is evidence that the regulation of personal health information impedes the provision of appropriate health services to individuals, we would caution against unnecessary amendment which may water down protections if the problem lies in the interpretation of the legislation rather than its current terms. A better solution in these circumstances might be a campaign of education to counteract misunderstandings concerning the operation of the legislation.

8–11 Does the *Privacy Act* provide an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent? Does the draft *National Health Privacy Code* provide a more appropriate and effective framework for handling health information in these circumstances?

In our view, the draft *National Health Privacy Code* provides a fuller, more specific regime for handling health information in circumstances where an individual has limited capacity to consent which offers a more appropriate and effective framework than the *Privacy Act.*

8–13 Should the *Privacy Act* be amended to allow health service providers to collect information about third parties without their consent in line with Public Interest Determinations 9 and 9A? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of such information than the current provisions of the *Privacy Act*?

Yes, given that these are ongoing issues, we are in agreement with the recommendations of the OPC Review that NPP 10 of the *Privacy Act* be amended to include an exception that mirrors the operation of Public Interest Determinations 9 and 9A.

8–14 Should the *Privacy Act* be amended to allow insurance companies to collect health information about third parties without their consent in similar circumstances to those set out in Public Interest Determinations 9 and 9A?

Yes, given the ongoing nature of this issue and the accepted legitimacy of this practice of life insurers gathering family history information for the purposes of insurance underwriting, it would seem appropriate for there to be an amendment to the *Privacy Act* to allow insurance companies to collect health information about third parties without their consent in similar circumstances to those set out in Public Interest Determinations 9 and 9A.

8–15 Should NPP 10 of the *Privacy Act* be amended to clarify when health information may be collected without consent? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of health information without consent?

We would be in support of an amendment to NPP 10 of the *Privacy Act* to clarify when health information may be collected without consent.

8–17 Is guidance by the Office of the Privacy Commissioner an appropriate and effective response to concerns that the phrases in NPP 2, 'primary purpose of collection' and 'directly related to the primary purpose', might impede the appropriate management of an individual's health? If not, what is an appropriate and effective response?

Our preferred approach is outlined below in response to para 8-18.

8–18 Does NHPP 2 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for the use and disclosure of health information than the current provisions of the *Privacy Act*?

Yes, we are of the view that this provides an effective model for the use and disclosure of health information and addresses the concerns that have been raised

about the NPPs that they might be interpreted in a way that impedes the provision of holistic health care and the appropriate management of an individual's health care.

8–20 Is the exception in NPP 6.1(b) in relation to providing access to health information (that is, that access may be denied if it would pose a serious threat to the life or health of any person) appropriate and effective? Should the exception be extended to allow a health service provider to deny access to health information if providing access to the information would pose a threat to the therapeutic relationship between the health service provider and the health consumer?

There is clearly a need for some exceptions to providing access to health information. However, an objection could be raised that this possibility of extending the current exception to allow a health a health service provider to deny access to health information if providing access to the information would pose a threat to the therapeutic relationship between the health service provider and the health consumer is somewhat paternalistic.

8–21 Do NHPP 6 and Part 5 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for access to health information than the current provisions of the *Privacy Act*?

In our view, NHPP 6 and Part 5 of the draft *National Health Privacy Code* do provide a more appropriate and effective framework for access to health information than the current provisions of the *Privacy Act.* This helps to illustrate the advantages of privacy principles dedicated to health information which ensure tailor-made solutions and permit a level of detail not otherwise possible.

8–22 Should the *Privacy Act* be amended to deal expressly with the situation in which a health service provider ceases to operate? Does NHPP 10 of the draft *National Health Privacy Code* provide an appropriate and effective framework to deal with this situation?

We are of the view that specific provision should be made in the *Privacy Act* to deal with the situation in which a health service provider ceases to operate. In this regard, NHPP 10 of the draft *National Health Privacy Code* would appear to provide an appropriate and effective framework to deal with this situation.

8–24 Does NHPP 11 of the draft *National Health Privacy Code* provide a more appropriate and effective framework to deal with the transfer of health information from one health service provider to another than the current provisions of the *Privacy Act*?

We are of the view that specific provision should be made in the *Privacy Act* to deal with the transfer of health information from one health service provider to another. In this regard, NHPP 11 of the draft *National Health Privacy Code* would appear to provide an appropriate and effective framework to deal with this situation.

8–25 Is the current public interest test in the *Privacy Act* and Section 95 and Section 95A Guidelines (that the public interest in promoting research

substantially outweighs the public interest in maintaining the level of protection of health information provided by the Act) appropriate and effective? If not, what is an appropriate and effective test?

We support the view put forward by a number of stakeholders referred to in the *Issues Paper* that it would be preferable to revamp the current approach (section 95 and section 95A applying to the public and private sectors respectively) and replace it with a single set of principles and a single set of guidelines regulating health information in the conduct of health and medical research. In this respect, the approach contained in the draft *National Health Privacy Code* appears to provide a more unified and effective approach. We also note that it contains a more qualified public interest test than that set out in sections 95 and 95 of the *Privacy Act* which in practice would be more workable in the interests of ensuring that beneficial research is not unduly impeded.

8–26 Should the term 'research' be defined for the purposes of the *Privacy Act*? If so, how should the term be defined?

This term is defined in the current *National Statement on Ethical Conduct in Research Involving Humans* and will be included in the revised *National Statement.* In addition, the *Australian Code for Responsible Conduct in Research* also provides guidance about the retention and privacy of research records. We do not believe it is necessary to include a definition of research in the Act. The general guidance principles for privacy are generally well understood now by researchers and human research ethics committees. In addition, the OPC has received reports in relation to SS95 and 95A guidelines issued under the *Privacy Act* (see Question 8-32). Whilst it is essential that research must also be an activity governed by privacy regulation, this is an activity that can be subject to the approach of high level general guidance with details in the *National Statement* and other research guidelines. The OPC should have power to audit and oversee these guidelines.

8–27 Should the *Privacy Act* be amended to include definitions of 'identifiable', 're-identifiable' and 'non-identifiable' personal information?

We note that the OPC Guidelines seek to provide some guidance as the interpretation of these terms. However, given the centrality of these concepts to the operation of the *Privacy Act* it would seem desirable for a definition of these terms to be expressly included in the legislation. In providing such definitions, it would be important, however, to ensure consistency with the definitions in the *National Statement* (once the final draft is settled) to avoid creating further confusion.

8–28 Should the *Privacy Act* draw a distinction between 'identifiable' and 're-identifiable' health information in the context of health and medical research?

Yes. This distinction is generally drawn in human research and included in the *National Statement.* Arguably, 'identifiable' and 're-identifiable' amount to the same effect and the distinction in privacy is more relevantly between identifiability and complete anonymity.

8–29 What provision should be made for the use of health information without consent in health and medical research?

Further to our submission above, we agree with the view put forward in the *Issues Paper* that the *Privacy Act* and the *National Statement* should be as consistent as possible. We are of the view that the coverage in the *National Statement* (second consultation draft) which provides a fuller, more detailed approach than NPP 2 to the use of health information in health and medical research without consent is an appropriate and effective model.

8–30 Does NPP 2 provide an appropriate and effective framework for the use, without consent, of health information in health and medical research?

See submission above.

8–31 Are Human Research Ethics Committees the most appropriate bodies to make decisions about the collection, use and disclosure, without consent, of health information in the context of health and medical research?

We are strongly of the view that Human Research Ethics Committees are the most appropriate bodies to make decisions about the collection, use and disclosure, without consent, of health information in the context of health and medical research. This model of ethical review, based on the collective wisdom of an interdisciplinary group, has proved in general to be very effective in practice. This is not to say, however, that it is not capable of improvement and we endorse the various recommendations that have been made by the ALRC/AHEC in the course of their joint inquiry into the protection of human genetic information for supporting and strengthening the ethical review process. We also endorse the specific recommendations made on the issue of waiver of consent and the need for greater consistency in interpretation of this power, and greater accountability in documenting and reporting on decision-making involving waiver of consent.

8–32 Are the requirements imposed on Human Research Ethics Committees by the Section 95 and Section 95A Guidelines issued under the *Privacy Act* appropriate and effective?

The original Section 95 was a late addition to the legislation as research was originally to have been considered outside the Act. The operation of these sections has caused difficulties for HRECs. Many were unaware that the original Section 95 only applied to Australian agencies and not privacy generally. Specific guidelines were prepared by the Australian Health Ethics Committee and these were gradually understood by HRECs with a system of reporting to the PC. These Section 95/95A guidelines include an important consideration for HRECs in considering whether to allow access. HRECs are required to weigh the public interest in decisions about releasing or accessing private information. Reviews of HRECs will be critical, but generally privacy should be an appropriate responsibility for checking and auditing by HRECs.

8–33 Does the *Privacy Act* provide an appropriate and effective regime for: (a) the establishment of health data registers; and (b) the inclusion and linkage of health information in data registers?

We wish to note our in principle support for the establishment and maintenance of health data registers which play an important role in seeking to reduce the incidence of disease and promote public health. However, as the NHMRC has noted, such registers raise significant privacy issues and there is a clear need for a rigorous ethical and privacy framework to ensure appropriate protection of the public interest. Consistent with our recommendations above about the need for separate treatment of health information from other sensitive information in the *Privacy Act,* we are of the view that the regulation of health data registers should also be dealt with separately. Moreover, further to the point raised in the *Issues Paper*, there needs to be clarification of the circumstances in which linkage of health data without consent may be permitted*,* to overcome the practice of some HREC to automatically reject proposals involving data linkage, evidently in the 'mistaken belief that such linkage is not ethically or legally acceptable.'

11. Developing Technology

11–4 Should the *Privacy Act* be technologically neutral?

Every effort should be made to preserve the technological neutrality of this Act.

13. Transborder Data Protection

13–1 Does NPP 9 provide adequate and appropriate protection for personal information transferred from Australia to a foreign country? Does the relationship between NPP 2 (disclosure of personal information) and NPP 9 (international transfer of personal information) need to be clarified?

We have some reservations about the adequacy and appropriateness of the protection of personal information transferred from Australia to a foreign country. In particular, we note the various criticisms that have been raised with regard to NPP 9 with a number of tests couched in terms of 'reasonableness' ('reasonable belief' NPP 9(a) and 'reasonable steps' NPP 9(b)) which are seen as weak and imprecise and fall short of the requirements in other jurisdictions, such as under the EU Directive. This all points to the need for the tightening up of the provision, as well as ensuring adequate guidance to stakeholders about what their obligations under NPP 9 entails (including which jurisdictions have substantially similar principles for the purposes of NPP 9(a)). We also support amendment of NPP 9 to clarify the relationship with NPP 2 to make it clear that the obligations under the Act with regard to disclosure of information outside of Australia apply to the release of personal information to organisations and government bodies as well as individuals.

13–2 Should the *Privacy Act* be amended to clarify that NPP 9 applies when personal information is transferred outside Australia to a related body corporate?

Yes, we are in support of such an amendment.

13–3 What role, if any, should the Office of the Privacy Commissioner play in identifying countries that have equivalent *Privacy Act* protection for personal information?

We support the OPC as the appropriate body to undertake the role of identifying countries with equal privacy protection. No doubt, the OPC will develop appropriate inter-governmental arrangements with DFAT. We believe that the OPC has, or should develop, the expertise to make such assessments.

13–4 Should organisations be required to inform individuals that their personal information is to be transferred outside Australia? If so, what form should such notification take?

We are of the view that organisations should be required to inform individuals that their personal information is to be transferred outside Australia as this would be relevant information to many people. As to the form such notification should take, we acknowledge the points raised in the *Issues Paper* about potential cost burden on businesses if individual notification were to be required. At the very least, this information should be included on the company website as part of the privacy statement of that organisation.

13–5 Is adequacy of the *Privacy Act* under the European Union Data Protection Directive: (a) necessary for the effective conduct of business with European Union members; and (b) desirable for the effective protection of personal information transferred into and out of Australia? If so, what measures are necessary to ensure the adequacy of Australia's privacy regime under the European Union Data Protection Directive?

We note that there is little evidence at present that the inadequacy of Australian's privacy regime for the purpose of the EU Directive is inhibiting trade between Australia and country members of the European Union. Nevertheless, we are of the view that Australia should, as a matter of principle, be striving to upgrade its privacy laws to ensure that it does match the standards in the EU Directive. If not immediately relevant for the purposes of fostering business, qualifying as adequate for the purpose of the EU Directive has important symbolic significance signaling that Australia takes privacy regulation seriously and seeks to promote best practice in this area.

13–6 Does the APEC Privacy Framework provide an appropriate model for the protection of personal information transferred between countries? Are other standards, such as the Asia-Pacific Charter, a more appropriate model?

We note that there are currently high standards contained in the current Asia-Pacific Privacy Charter. We are aware that the EU Directive has been influential in the development of our NPPs. We consider that we should establish best international practice in our standards and these should be consistent with not only the EU standards but also the APEC and Asia-Pacific standards as all these regions are major trading and business points.