SUBMISSION TO THE SENATE REFERENCE COMMITTEE

RE THE

INQUIRY INTO THE *PRIVACY ACT* 1988 (CTH)

FROM

PROFESSOR MARGARET OTLOWSKI,

PROFESSOR DON CHALMERS,

DR DIANNE NICOL AND

PROFESSOR LOANE SKENE

FROM THE

CENTRE FOR LAW AND GENETICS

UNIVERITIES OF TASMANIA AND MELBOURNE

FEBRUARY 2005

Consistent with the Centre for Law and Genetic's program of research and activities, the focus of this submission is on privacy issues in relation to genetic testing, however, brief attention is also given to the issues raised by 'Smart Card' technology, drawing on the experience of one of our members (Dr. Dianne Nicol) acquired from teaching Information Technology Law.

As the issues raised by this Inquiry of the Senate References Committee intersects with a number of other inquiries and processes with which members of the Centre have been involved, it may be helpful if we put this submission in some context. In particular, we refer to the major inquiry jointly undertaken by the Australian Law Reform Commission and the Australian Health Ethics Committee of the NHMRC into the protection of human genetic information, which culminated in a 2 volume report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (2003). A major thrust of this inquiry and the ensuing recommendations was on privacy issues in relation to genetic testing and potential for discriminatory use by third parties of the information obtained. Members of the Centre of Law and Genetics have worked closely with the Australian Law Reform Commission in connection with this reference either as members of the Commissioner's Advisory Committee and/or as Consultants. The Centre also made detailed submissions to the Inquiry's initial Issues Paper and the Discussion Paper. The parts of these submissions that relate to privacy are attached. We broadly support the recommendations that the *Essentially Yours Report* makes for reform in Australia to better protect the privacy of genetic information and to protect against unfair discriminatory use of such information by third parties.

In relation to the specific matters referred to the References Committee, we offer the following submissions

(a) the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians, with particular reference to

…

(ii) the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy including:

- **'Smart Card' technology and the potential for this to be used to establish a national identification regime**

As with many other aspects of the information technology revolution, smart card technology has the capacity to offer significant benefits to consumers. Smart cards have countless applications. They can be used as health cards, phone cards, transport cards, financial transaction cards, customer loyalty cards, utility recharge cards and so on. It has been estimated that more than one billion smart cards have been issued per year since 1998. But as with other areas of electronic commerce, smart card have the capacity to record large amounts of personal information about individuals and hence pose significant privacy issues. In some regards, these issues are no different from those raised in any other area in which personal information is collected. However, the sheer volume and nature of the information collected and stored in a single smart card raises particular issues, which have the capacity to pose unique privacy concerns and to affect consumer confidence in the technology. As the OECD Working Party on Information Security and Privacy has stated, for such technology to be trustworthy, infrastructures and services must be reliable, transactions must be secure and private, and personal data must be effectively protected. Many of these matters can and should be dealt with through the technology itself, using such tools as disabling and circumventing mechanisms, adequate encryption and other privacy-related tools. The smart card industry is also aware of consumer concerns in this area and has its own codes of conduct. One example is the Asia Pacific Smart Card Forum, which was established in 1995 to promote smart card industry in Australia. The Forum has developed a code of conduct, which requires compliance with the NPPs.

Appropriate and adequate privacy legislation is also an essential element in protecting consumers from misuse of personal information and alleviating consumer concerns. One matter that particularly needs to be looked at is the definition of personal information. The definition in its current form focuses on traditional forms of information collection. In the modern information technology environment vast amounts of data can be collected about an individual that does not necessarily fit within the existing definition. Individuals leave 'pools' of data about themselves whenever they enter into the electronic environment. These pools, when collected together, have the capacity to reveal significant information about an individual: their interests, shopping habits, financial transactions and so on. The definition of personal information may need to be updated to deal with these new methods of collecting information. In this regard, the word of Justice Michael Kirby are instructive. In his article "Privacy in Cyberspace" (1998) 21 *UNSWLJ* 323 he noted that:

> [t]here has been little endeavour to reflect the major scientific and technological developments of the last fifty years, and their impact on human rights, in a conceptual way. Instead, old human rights instruments developed for earlier times are scrutinised for their possible utility in solving controversies presented by the new technology. Piece-meal legislation is enacted. No Luther of jurisprudence has emerged to pull together the implications of nuclear physics, informatics and biotechnology for twenty first century man or woman.

Justice Kirby went on to suggest that we also need to examine the need for a second generation of privacy principles such as:

- a right not to be indexed;
- a right to encrypt personal communications effectively

- a right to fair treatment in public key infrastructures, so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy;
- a right to human checking of adverse automated decisions and a right to understand such decisions;
- a right – going beyond the openness principle, of disclosure of the collections which others have access to and which might affect the projection of the profile of the individual concerned.

We support Justice Kirby's views in this regard and suggest that the time is now ripe, seven years after he made these comments, to explore mechanisms for updating our privacy laws to reflect new technological developments.

• genetic testing and the potential disclosure and discriminatory use of such information

There is no doubt that the increased availability of genetic testing, the resulting collections of genetic samples, and overall proliferation of genetic information has created significant challenges for privacy regulation. Although genetic information is clearly a form of health information, it does have a number of particular features the cumulative effect of which arguably justify special protection of genetic information, at least in some circumstances. These include its familial nature, its highly personal and sensitive quality, its probabilistic aspect (at least in the context of *predictive* genetic testing), and the potential for discriminatory use, against the interest of the person to whom the information relates. Further, it logically follows that if genetic information ought to be protected, so too should the genetic samples from which such information can be obtained. It is our submission that a targeted legislative response to these issues is required details of which are outlined immediately below.

(iii) any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way

From the outset, we wish to acknowledge that the expansion of privacy protection under federal legislation to the private sector was a significant step forward and has forced a shift in culture amongst organisations in Australia towards the handling of personal information. It has also been significant in ensuring that Australian privacy standards are brought into compliance with international standards. Difficulties, however, remain as a result of the fragmented nature of health privacy laws in Australia including differences in coverage between the public and private sector under the federal legislation and there are significant gaps in coverage, with, for example, state government agencies and universities falling outside the scope of the federal legislation. This is potentially problematic given that most genetic research in Australia is conducted in universities and public hospitals. State and territory regulation of this area is incomplete and lacking in uniformity. Not all jurisdictions have such legislation (Tasmania, for example, has only recently come on board and the legislation is yet to commence) and where such legislation exists, it is not necessarily compatible with either the public or private sector provisions in the federal *Privacy Act 1988* (Cth).

Further, the enforcements mechanisms contained within the *Privacy Act 1988* (Cth) are relatively weak. The federal privacy regime is complaints-driven and conciliation-based. In the first instance, health consumers have to be aware of their rights to be in a position to understand that they can bring a complaint under the legislation. Assuming that they are aware and do lodge a complaint, the processes for dealing with complaints under the legislation involves considerable compromise of interests. Although there are clearly advantages with a conciliated approach over litigation, and the ‘soft touch’ approach has no doubt been helpful in getting private organisations on board, the rights of aggrieved individuals are limited under the existing legislation because in the event that orders are made by the Privacy Commissioner, such orders can only be enforced by court action. States and territories are now increasingly introducing their own privacy legislation, in some instances specific to protecting the privacy of health records. (See, for example, the Victorian *Health Records Act* (2001), the New South Wales *Health Records and Information Privacy Act 2002*, and the Tasmanian *Personal Information Protection Act 2004* (yet to be commenced).

With regard to privacy protection for genetic information in particular, and health information more generally, we support the need for harmonisation of information and health privacy legislation. ‘Health information’ is recognised under the *Privacy Act 1988* (Cth) as a ‘sensitive’ category of information, which therefore requires particular protection. For obvious reasons, the requirements of the National Privacy Principles (NPPs) are most rigorous in relation to sensitive information, for example, NPP 10 imposes restrictions on whether and how an organisation can collect health information about an individual and NPP 2 imposes stricter limits on how sensitive information may be used or disclosed than is the case for non-sensitive personal information. Genetic information is not specifically referred to in the *Privacy Act 1988* (Cth) but it would come within the definition of health information. This has been confirmed by the Privacy Commissioner’s guidelines although questions have arisen as to whether carrier genetic testing relates to the ‘health or disability of an individual’ as defined in s 6(1).

As indicated above, we endorse the recommendations in the ALRC/AHEC *Essentially Yours* Report for enhancing the protection of privacy and protecting against illegitimate disclosure and potential discriminatory use, in particular, the:

- proposed amendment of the objects and definition sections of the *Disability Act 1988 (Cth)* to more clearly encompass genetic discrimination;

- proposed raft of recommendations in relation to the insurance and employment sectors to protection against unfair discriminatory use of genetic information;

- proposed amendment of the *Privacy Act 1988* to include genetic samples as information;

- proposed creation of a criminal offence in respect of testing of a person’s genetic sample without that person’s consent or other legal authority;

- proposed creation of the standing body to advise government (Human Genetics Commission of Australia);

- proposed harmonisation of information and health privacy legislation as it relates to human genetic information.

We note that the ALRC/AHEC *Essentially Yours* recommendations were limited to harmonisation of information and legislation as it relates to human genetic information but this was due to constraints arising from the Inquiry’s terms of reference. Indeed, the ALRC/AHEC Inquiry is on the record as supporting an integrated approach whereby any difficulties arising in respect of genetic information are dealt with in the wider context in which they arise rather than implementing specific legislation for the protection of genetic information/samples. It is entirely consistent with this approach for protection for genetic information and samples to be encompassed within legislation dealing with the protection of health information generally. Enacting specific legislation dedicated to health information would allow the privacy standards to accommodate the particular characteristics and generally sensitive nature of this information. This would still allow scope for developing particular provisions within that legislation recognizing the special nature of genetic information, and related issues such as the ‘right not to know’ and disclosure of genetic information to blood relatives. It avoids assumptions, however, about such information being uniquely sensitive and would allow for special provision to be made for protection of other particularly sensitive health information.

In regards to the last of the above dot points, we note the work already underway of the Australian Health Ministers’ Advisory Council in respect of a National Health Privacy Code governing the handling of all health information. Whilst we support the intentions behind the proposal for a National Health Privacy Code, we do not believe that this goes far enough and significant obstacles exist to securing uniform application and enforcement. This Code is not envisaged to take effect directly as legislation, but rather the Code would take effect under Part IIIAA of the *Privacy Act 1988* (Cth). This would enable regulations to be made under the Act prescribing an instrumentality of a state or territory as an organisation for the purposes of the Act and through this means, the operation of the Code could be extended to the state and territory public sector health providers. This non-legislative status, in turn, raises difficult issues in relation to implementation and enforcement. For the information of the Committee, we are attaching a brief submission which Professor Otlowski and Dr Nicol made to the Australian Health Minister’s Advisory Council (AHMAC) in relation to the National Health Privacy Code (Draft) Consultation Paper which addresses these issues (note that we have been unable to find any details as to the progress of this Code, either on the AHMAC website or elsewhere). In our view, a legislative response is needed, most likely requiring the co-operation of the Commonwealth and states and territories. Only in this way can the problems of application and enforcement be overcome.

In summary, we believe that it is of the utmost importance to ensure the appropriate protection of genetic information and genetic samples from which such information can be obtained and to protect against potentially discriminatory use that the ALRC/AHEC *Essentially Yours* recommendations are implemented.

(b) the effectiveness of the *Privacy Amendment (Private Sector) Act* 2000 in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness

Whilst, as noted above, we welcome the initiative to expand privacy protection in Australia to the private sector, we have some concerns about the weak enforcement capacity of the legislation. We are also of the view that the exemption given to employers under the legislation is not justified. More detailed argument in relation to concerns about the employee records exemption are set out in a paper by Professor Otlowski, published by the *Australian Journal of Labour Law,* which is attached. We note that the ALRC/AHEC *Essentially Yours* Report's recommendations for the employment sector included a recommendation that the Commonwealth should amend the *Privacy Act 1988* (Cth) to ensure that employee records are subject to the protection of the Act to the extent that they contain genetic information (Recommendation 34-2). The limited terms of this recommendation stem from the Inquiry's Terms of Reference; it is clear from the commentary and the recommendation which follows that the Inquiry's preferred position is that the reforms should be wider, encompassing all health information (Recommendation 34-2).

ATTACHMENTS

1. Centre for Law and Genetics**,** Submission to the Australian Law Reform Commission and Australian Health Ethics Committee Joint Public Inquiry, *Protection of Human Genetic Information Issues Paper* (January 2002) Chapter 4: Privacy
2. Centre for Law and Genetics**,** Submission to the Australian Law Reform Commission and Australian Health Ethics Committee Joint Public Inquiry, *Protection of Human Genetic Information Discussion Paper* (December 2002) Chapter 7: Information and Health Privacy Law
3. M. Otlowski and D. Nicol, Submission to the Australian Health Ministers' Advisory Council, *National Health Privacy Code (Draft) Consultation Paper* (April 2003)
4. M.Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169-176

(Attachment 1)

SUBMISSION

TO THE JOINT AUSTRALIAN LAW REFORM COMMISSION AND AUSTRALIAN HEALTH ETHICS COMMITTEE PUBLIC INQUIRY

PROTECTION OF HUMAN GENETIC INFORMATION

Issues Paper

Chapter 4: Privacy

January 2002

DRC CHALMERS, M OTLOWSKI AND D NICOL
CENTRE FOR LAW AND GENETICS

Chapter 4: Privacy

4-1 Is the framework provided for privacy protection in the federal Privacy Act adequate to protect genetic information? If not, why not, and how might the existing framework be improved?

Genetic information has particular features that create troublesome issues in relation to information privacy. Perhaps the two most prominent features are the familial nature of genetic information and the capacity to re-identify the personal genetic information contained in a tissue sample after de-identification.

Whilst the framework provided for privacy protection under the federal *Privacy Act* probably does provide adequate protection in the health setting we do have some concerns with the use of genetic information in the research setting. Most genetic research in Australia is conducted in universities and public hospitals, although there is an increasing trend for the private sector to be involved in this research, either by funding university and hospital researchers to conduct the research or by conducting its own research.

Public hospitals and universities are generally considered to be State and Territory government agencies and therefore come within the ambit of State and Territory privacy laws. The privacy legislation within the various States and Territories is incomplete and lacking in uniformity. In Tasmania, for example, there is no privacy legislation (although a draft Bill is currently being considered, with the release of Tasmanian Information Privacy Legislation Issues Paper in November 2001). Where privacy legislation does exist, it is not necessarily compatible with either the public sector or private sector provisions in the federal Act.

We note that, where public hospitals and universities receive public funding, they will be governed by NHMRC guidelines. The increasing commercialisation of genetic research means that this will not always be the case. One issue that needs to be addressed is whether a university researcher receiving private sector funding is governed by state law or by the federal private sector requirements.

A private company conducting its own research will generally be covered by the federal private sector provisions. If the company falls within the definition of a small business it will not be exempt from the private sector requirements if it is a health service provider or if it is dealing with health information. A health service is defined in s6(1) as:

> ‘(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
>
> (i)to assess, record, maintain or improve the individual’s health; or
>
> (ii)to diagnose the individual’s illness or disability; or

> (iii) to treat the individual's illness or disability or suspected illness or disability; or
>
> (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.'

In our view, research undertaken by a genomics company would not fall within the definition of a health service, at least in the general sense. This conclusion is supported by the fact that private sector research organisations are not listed as health service providers in the Privacy Commissioner's *Guidelines on Privacy in the Private Sector* at A2.1.

Health information is defined in s6(1) as:

> '(a) information or an opinion about:
>
> (i)the health or a disability (at any time) of an individual; or
>
> (ii)an individual's expressed wishes about the future provision of health services to him or her; or
>
> (iii) a health service provided, or to be provided, to an individual;
>
> that is also personal information; or
>
> - other personal information collected to provide, or in providing, a health service; or
>
> (c)other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.'

Arguably genetic information used in the research context is information about the health of a person or information collected in connection with the donation of body parts, etc. The Privacy Commissioner considers that health information includes genetic information, when this is collected or used in connection with delivering a health service, or genetic information when this is predictive of an individual's health. This does not overly assist in determining whether genetic information used in the research context is health information. The situation is much more clear in relation to predictive genetic test information, which will generally fall within the ambit of health information.

There is a preponderance of small biotechnology companies and small subsidiaries and shelf companies associated with foreign companies in Australia. We are aware that human tissue collected in public institutions has been transferred to biotechnology companies. This human tissue, of its nature, contains identifiable or potentially identifying information about the donor. We are of the view that the position in relation to genetic research requires clarification. The *Privacy Act* could be amended to ensure that the health information provisions extend into the research setting.

We wish to make one further submission in relation to this question in relation to employee records. Whilst an exemption for employers in respect of employee records has been adopted under the Commonwealth private sector legislation, the approach has been sharply criticised from a number of quarters, including the House of Representatives, Standing Committee on Legal and Constitutional Affairs when it reviewed the

Commonwealth Private Sector Bill. The stated rationale for the exemption is that privacy protection for employee records is properly a matter for workplace relations legislation. The reality is, however, that for the majority of worker in Australia there is little tangible protection of the privacy of their employment records (see further our comments in response to question 10-7).

4-2 Does the higher level of protection afforded to `sensitive information' (including health information) under the Privacy Act adequately cover all forms of genetic information?

The higher level of protection afforded to 'sensitive information', including 'health information', under the *Privacy Act* as amended, does appear to cover most types of genetic information that one would reasonably expect to be included within the health context. However, there may be gaps in the research context (see above at 4-1). Most importantly, it clearly covers genetic information obtained through predictive genetic testing which is a major area of concern in relation to privacy protection, as well as genetic information gained through diagnostic and prenatal testing. We would also agree with the view expressed at para 4.77 of the *Issues Paper* that personal information derived from genetic testing that is provided to insurers or employers would constitute health information, even though it is not taken for clinical or therapeutic purposes.

While we accept that there may be some debate as to the appropriate interpretation of the reference to information about the 'health (or disability) of an individual…' in s 6(1) of the Act, we believe that the definition of health information should not be so narrowly interpreted as to exclude carrier testing on the basis that this is not information about a person's health. Further, we note that the definition of health information referred to in the Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector* cited at para 4.76 of the *Issues Paper* states that 'health information includes' and does not purport to be exhaustive. As carrier testing has implications for an individual's procreative choices (including whether or not IVF treatment may be required), it would be surprising indeed if this were not covered by the definition of health information, even though it does not directly pertain to the individual's own health. In light of the doubts that have been raised about this matter, it may be useful to put this question, as a matter of interpretation, to the Federal Privacy Commissioner. We are certainly of the view that it is important that this category of genetic information is afforded the same level of protection as other forms of genetic information, particularly as there has already been evidence in some jurisdictions of adverse treatment of individuals on the basis of their carrier status.[1]

We do not, however, have any difficulty with the conclusion that genetic testing for the purposes of establishing paternity or for forensic purposes is not health information for the purposes of the legislation.

---

[1] **Billings P., *et al*, 'Discrimination as a Consequence of Genetic Testing' (1992) 50 *American Journal of Human Genetics* 476.**

In summary, we are reasonably confident that the coverage of the legislation is sufficiently broad to encompass most relevant forms of genetic information in the context of predictive genetic testing. However, in the event that gaps in coverage are identified, they should be addressed, by legislative amendment of the definition if necessary.

4-3 Are there any potential privacy problems that arise in the practical application of the Privacy Act and the National Privacy Principles to:

the collection of genetic samples and information?
the use and disclosure of genetic samples and information?
access by individuals to genetic samples and information relating to them?
the de-identification of genetic samples and information?
other aspects of genetic information privacy?

Although generally the provisions relating to the collection of genetic samples and information appear adequate, we would like to see clarification of the circumstances in which genetic samples and information can be collected for research purposes without the consent of the donor. In what sort of circumstances would consent be impracticable? When would de-identified information not be suitable? Because consent is such a fundamental requirement in the conduct of research involving genetic information, permission to waive the consent requirements should not be granted lightly.

The situation becomes more complicated when it is intended to use or disclose genetic information for secondary purposes. The question of what a person would reasonably expect becomes critical.

Although the privacy principles allow an individual to access information relating to them, they have to know in the first instance that the information has been collected and stored. NPP 1.3 requires that an individual is given certain information about personal information collected about them. Where information is collected with consent, the individual will generally be informed about the issues listed in NPP 1.3 at the time when consent is sought. When information is collected without consent in circumstances where it would be impracticable to obtain consent, it is difficult to see how an individual could be informed as to the matters listed in NPP 1.3. This reinforces the need for particular attention to be paid to the circumstances in which the consent requirement should be waived.

An additional difficulty with genetic information is that, although it may be collected from one person, it is personal information about a range of people (anyone with a direct family connection). The privacy principles do not provide guidance as to the extent of the notification requirement. Unless a person knows that information has been collected about them, the access provisions become meaningless.

In relation to the issue of de-identification, there are particular problems with the de-identification of genetic information in tissue samples. Because a sample can be re-identified, the only way to permanently de-identify a sample is to physically destroy it. There may be some justification for requiring this to be done once the relevant genetic information has been extracted.

4-4 What particular issues arise from the application of privacy law to the protection of human genetic samples and information? For example:

> Is the familial nature of genetic information adequately recognised in privacy principles applying to the collection and disclosure of genetic information?
> Are the interests of individuals who prefer `not to know' about genetic information relating to them adequately protected?

One of the main shortcomings of the privacy legislation's coverage of genetic information is that it fails to give recognition to some of the particular characteristics of this form of information: foremost amongst these is the familial nature of genetic information and the fact that much of this information is predictive only and many individuals will elect not to undertake testing, or even if they do, will not want to know the results of those tests.

As genetic information is afforded no special status under the *Privacy Act*, as amended, standard rules regarding the disclosure of health information apply, strictly limiting those to whom such information can be disclosed. This is one example of how this legislation, which is of general application and not specific to genetic privacy, may not always be ideal in its application to genetic information. There is growing support for the view that familial nature of genetic information demands some modification of the usual principles in relation to privacy and non-disclosure and that information should be shared with family members whose health may benefit from access to this information.[2] In this respect, the new privacy regime (in particular, NPP 2.1(e)) arguably applies too stringent a test, precluding disclosure in circumstances where it may be beneficial to family members, alerting them to the risk of genetic disease and perhaps enabling them to institute preventative or therapeutic strategies.

Another concern about the inappropriate application of the privacy principles in the context of genetic test information relates to the protection of those individuals who choose not to know about genetic information relating to them.

The right of an individual not to know abut genetic information relating to them is supported in a number of international instruments[3] and plays an important role in relation to this form of predictive information. Significantly, it receives no special

---

[2] **L. Skene, 'Patients' Rights or Family Responsibilities? Two Approaches to Genetic Testing' (1998) 6 *Medical Law Review* 1.**

[3] **Council of Europe, *Bioethics Convention on Human Rights and Biomedicine,* Article 10; UNESCO, *Universal Declaration on the Human Genome and Human Rights,* Article 5.**

recognition under the *Privacy Act*, however, this is unsurprising in light of the general nature of this legislation. Not only is there no specific recognition or protection of the right not to know, there are provisions contained in the Act (in particular, NPP 1.5) which may encourage information to be inappropriately disclosed to the individual about whom it is collected in an over zealous attempt to comply with the requirements of the legislation.

It is vitally important that the right not to know is afforded appropriate protection under privacy legislation to ensure that the potential arising from the availability of genetic information does not become an unwanted burden.

4-5 Does the federal Privacy Act provide an adequate framework for national regulation of health information privacy and, if not, why not?

The federal Act does not provide an adequate framework because there are gaps in the privacy regime it creates. In particular, the federal Act does not cover public hospitals and universities, as discussed under question 4.1. A large proportion of genetic information collected in Australia is probably held by these institutions. Ideally, all organisations and institutions collecting and using genetic information should be subject to the same or similar privacy obligations.

4-6 Should there be uniformity or greater harmonisation of federal, state and territory laws concerning the privacy protection of human genetic information?

Although there is negligible specific coverage of genetic privacy in Australia (in fact Victoria is the only jurisdiction to have enacted privacy legislation which expressly covers genetic information[4]), there is quite a patchwork of coverage of general privacy legislation which has application to genetic information as a form of health information. The present situation, which involves considerable duplication of effort between the federal public and private sectors, (as well as state and territory legislation) is complex and confusing. Although there are many similarities between the public and private sector regimes, there are also some significant differences which are not always justifiable. Difficulties will inevitably arise in some cases in determining whether certain health information falls within the public or private sector regimes, or possibly both might apply to different aspects of the same information. Rationalisation, with a view to achieving uniformity, or at least greater harmonisation of the present legislative patchwork would obviously be desirable. This would instill greater clarity and certainty into the law and would also help to promote awareness of the need to properly protect the privacy of genetic information.

---

[4] ***Health Records Act* 2001 (Vic).**

4-7 Would any deficiencies identified in the privacy protection of genetic information best be addressed through:

amendments to the existing privacy laws; or
the enactment of privacy legislation specifically dealing with all forms health information privacy legislation; or
the enactment of privacy legislation specifically dealing with only genetic information?

The existing privacy laws are complex and unwieldy, and there is already considerable dissatisfaction with the *Privacy Act's* coverage of health information. The solution to address deficiencies in the privacy protection of genetic information is definitely not to amend through adding to the legislation's scope, but rather, to remove the whole area of health information from the coverage of the legislation.

The best option for addressing deficiencies identified in the privacy protection of genetic information would be through the enactment of privacy legislation specifically dealing with all forms of health information. Enacting special legislation dedicated to health information allow the tailoring of privacy standard to accommodate the particular characteristics and highly sensitive nature of this information. This approach has already received support from the House of Representative, Standing Committee on Legal and Constitutional Affairs[5] and has been given in principle approval by the Government.[6] The Standing Committee's report acknowledged the complexity of privacy issues in health and the many concerns that had been raised about the inclusion of health provisions in the legislation. The committee also accepted that there were factors particular to health that make the idea of separate legislation or a separate compulsory and enforceable code attractive. Further, the committee commented on the difficulties arising from the differential coverage of health privacy within the public and private sectors. Indeed, the only reason that the committee ultimately decided to recommend that health information should remain part of the Bill, was because it thought it unlikely that a consensus could be achieved in the near future that would lead to the development of a separate legislative or regulatory code governing health services. Its recommendations were, instead, directed towards achieving such reforms in the future and therefore retaining the legislation's coverage of health information, at least on an interim basis, to ensure an acceptable level of privacy and access rights throughout Australia.

A useful model for health privacy legislation is the Victorian *Health Records Act* 2001 (Vic). Significantly, the Victorian legislature has deliberately enacted this health privacy legislation alongside general privacy legislation, thus reflecting the view that health information needs to be dealt with separately.

---

[5] ***Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*** **(2000) Chapter 6.**

[6] ***Government Response, House of Representative Standing Committee on Legal and Constitutional Affairs Advisory Report on the Privacy Amendment (Private Sector) Bill 2000,*** **Recommendations 14 and 15.**

Within the framework of privacy legislation specific to health, provisions could be included giving special recognition to the protection of genetic information to address perceived deficiencies in this area, as indeed could be done for other areas of health where there may be a need for particular protection. After all, genetic information is clearly health information and is best dealt with within this context, with the addition of specific provision as appropriate/ This would ensure a coherent approach is taken to the issue, in a manner consistent within a general health privacy framework.

This approach has the advantage of being able to afford appropriate protection to genetic information, but at the same time, avoiding an overreaction to the difficulties, and claims of genetic exceptionalism.

(Attachment 2)

SUBMISSION

TO THE JOINT AUSTRALIAN LAW REFORM COMMISSION AND AUSTRALIAN HEALTH ETHICS COMMITTEE PUBLIC INQUIRY

PROTECTION OF HUMAN GENETIC INFORMATION

DISCUSSION PAPER

Chapter 7: Information and Health Privacy Law

DECEMBER 2002

DRC CHALMERS, M OTLOWSKI AND D NICOL
CENTRE FOR LAW AND GENETICS

7. Information and Health Privacy Law

Proposal 7–1. As a matter of high priority, Commonwealth, state and territory governments should pursue the harmonisation of information and health privacy legislation as it relates to human genetic information. This would be achieved most effectively by developing nationally consistent rules for handling all health information.

As stated in our previous submission, we strongly believe that there is a need for greater harmonisation in privacy laws across Australia. We support Proposal 7-1. The Draft National Health Privacy Code provides a useful statement of intent by state, territory and federal health ministers to be bound by a consistent set of rules for handling all health information. However, it remains to be seen whether these rules will be adopted in all jurisdiction. The suggested mechanism for implementation of the Code under Part IIIAA of the *Privacy Act* is a sensible option, provided that it can be achieved.

We do maintain our view that the best option would be to have nationally consistent health privacy legislation. However, we recognise that it may be beyond the terms of reference of the inquiry to make this recommendation.

Proposal 7–2. The *Privacy Act 1988* (Cth) should be amended expressly to: (a) define personal information to include bodily samples from an individual whose identity is apparent or can reasonably be ascertained from the sample; and (b) define a 'record' to include a bodily sample.

We strongly support this Proposal. By defining samples in terms of personal information they are brought into an existing and workable regulatory scheme.

There is some academic support for the view that genetic samples are information, or, more likely, that they are records containing information. On this basis, samples would be interchangeable with the information they contain. Technologies such as bioinformatics are firmly establishing the linkage between computer technology and genetic technology and it is likely that human tissue samples will, over time, be seen increasingly as living databases of information. However, this stage has not yet been reached and the argument remains speculative. There is sufficient uncertainty about this argument at the present time to justify clarification through amendment of the Act.

Although privacy protection exists in relation to most genetic information (recognising that there may need to be some amendment to the definition of health information to ensure that it covers all genetic information), we believe that it is necessary to extend this protection to genetic samples. This will ensure that all of the people who come into possession of genetic samples are bound by privacy obligations, irrespective of whether or not they, themselves, extract genetic information. This will improve the capacity to keep track of the use and transfer of genetic samples from the source to the end user of genetic information. We recognise that research conducted using a genetic sample must be in accordance with the *National Statement*, as well as the NPPs or IPPs if it involves the collection or use of personal information. However, the section 95 and 95A provisions in the *Privacy Act* and the waiver of consent provisions in the *National Statement* do allow for use without consent in certain circumstances. The inclusion of genetic samples in the *Privacy Act* provides an additional layer of protection to sample providers.

It is appropriate that the sample collector should be under an obligation to explain the purpose of collection, primary and related secondary uses, the persons to whom the samples are usually transferred, access rights etc at the time of collection of the sample. This is consistent with the obligations of researchers to explain *future uses* of genetic information when conducting human genetic research. If these matters are properly explained to sample providers, growing concerns about the use of samples may well be alleviated. Moreover, the perceived need for samples to be accorded property status in order to protect the rights of sample providers may be rendered unnecessary. In many respects the protection afforded by the NPPs and IPPs is precisely the type of protection sought by advocates of property rights (as discussed in Chapter 17). In our view, these requirements will not impose an unreasonable burden on sample collectors. In the existing climate, with increasing concerns about personal privacy and increasing capacity to extract personal information from genetic samples, it makes good sense that sample providers should be told about what happens to their samples after removal. In many instances, all that may be required is for the sample provider to be notified that their sample will be stored for a particular period and then destroyed.

Importantly, the proposed mechanism for providing privacy protection for samples is relatively simple to establish. All that it requires is some minor amendments to the definitions in the *Privacy Act* and to the NPPs and IPPs. In contrast, the creation of a regime for the protection of samples based on property notions will be complex. A property regime will requires the creation of new *sui generis* legislative provisions (possibly included in the human tissue legislation in the states ans territories) or await an appropriate case argued and decided in the courts (and, within the vicissitudes of the common law, decided in such a way as to provide authoritative guidance on future conduct). However, none of these approaches is exclusive. The *Privacy Act* approach does not foreclose future development of a common law approach to the body as property. Perhaps this should be stated expressly in the Final Report.

We note that bodily privacy is protected indirectly and to a limited extent by the tort of trespass and by the duty of confidentiality. Although the High Court refused to recognise a tort of invasion of privacy in the case of *Australian Broadcasting Corporation v Lenah Game Meats*, in our view the court did not rule out the possibility of recognising such a tort in future cases. For example, Gummow and Hayne JJ said at para 107: '*Victoria Park* does not stand in the path of the development of such a cause of action'. Kirby J also pointed out that 'more was read into the decision in *Victoria Park* than the actual holding required' (at para 187). The judgments of the other judges could also be read as supporting the development of such a tort. The particular difficulty in the instant case was that Lenah Game Meats was a corporation and hence was not the sort of legal person that would be protected by such a tort. As such, it may be that we will have a tort of invasion of personal privacy in the future and this tort may apply when bodily samples are used in a way that is contrary to the dignity of the sample source. However, the possibility that a tort of invasion of privacy may be developed in the future should not be used as an argument against the inclusion of provisions for the protection of genetic samples in the *Privacy Act.*

In our view, the one major drawback of the proposed privacy regime is that enforcement powers are relatively weak when compared with common law actions. The privacy regime is complaints-driven and conciliation-based. Orders of the Privacy Commissioner can only be enforced by court action. However, we do recognise that there are many advantages of conciliation over litigation.

The inclusion of genetic samples within the definition of personal information will create obligations with regard to *new* samples, collected after the amendment Act enters into force. For this reason, there will still be gaps in the protection of providers of samples already in existence. We recognise that the proposed amendments to the *Privacy Act* do appear to provide a reasonable solution to the problems associated with collection and use of future genetic samples. However, we are of the view that it is necessary to consider other avenues for oversight of the use of existing genetic samples, particularly when they are stored in databases linked to other identifying information (see our submissions relating to Chapter 15).

We note that the implications of including genetic samples within the definition of personal information will need to be explored fully. One issue that springs to mind relates to cell lines, which fall into the category of genetic samples because they retain the DNA of the provider of the original cells. If the provider is reasonably identifiable, the privacy principles will apply to successive generations of cells. This conclusion has a number of implications, including one relating to the patenting of cell lines and other inventions based on human tissue where the donor is reasonably identifiable (the Mo cell line, derived from John Moore's spleen cells,[7] is one example). If cell lines are required to be deposited to fulfil the description requirements in the *Patents Act* 1990 (Cth), then, pursuant to NPP 2, sample providers would need to be advised of the transfer of their genetic sample to the Patent Office. This could be used as an indirect means of creating a requirement that sample providers consent to patenting of inventions based on their samples.[8]

As our final point, we wish to raise one concern that is linked to our comments in relation to Proposal 7-1. Some of the major collectors of genetic samples are universities and public hospitals. They are governed by state and territory legislation. Unless there is uniform or complimentary privacy legislation in all jurisdictions or a nationally consistent code, the advantages of this Proposal will be significanlty reduced.

---

[7] The subject of dispute in *Moore v Regents of the University of California* 51 Cal 3d 120 (1990).

[8] The issues associated with consent to patenting are canvassed more fully in D. Nicol, M. Otlowski and D. Chalmers, 'Consent Commercialisation and Benefit Sharing' (2001) 9 *Journal of Law and Medicine* 80.

Question 7–1. Does the *Privacy and Personal Information Protection Act 1998* (NSW) provide an appropriate model for amending the *Privacy Act* to include bodily samples within the definition of personal information?

We are of the view that it is desirable to maintain internal consistency within the *Privacy Act.* Consequently, our preferred option is for minor amendments to be made to the NPPs and IPPs to ensure that they apply to genetic samples as well as genetic and other personal information.

Question 7–2. What are the implications of Proposal 7–2 for the operation of the existing audit, investigation, complaints handling and enforcement provisions of the *Privacy Act*?

Question 7–3. If the *Privacy Act* were amended to cover genetic samples, what problems, if any, might arise in the relationship between that Act and other laws relating to bodily samples, such as the Human Tissue Acts?

There may be overlap between the provisions in the *Privacy Act* relating to bodily samples and other laws, including the Human Tissue Acts, the tort of invasion of privacy (should one be created in the future by the High Court), property law (see submissions relating to Chapter 17) etc. However, in our view the overlap does not create inconsistencies. It is important to provide adequate coverage with no gaps and therefore the fact that there may be overlap does not preclude the proposed extension of the *Privacy Act*.

We affirm our view that all human tissue is potentially re-identifiable, particularly as the number of genetic profiles stored in databases increases.[9] Whilst there are some similarities between genetic profiles, fingerprints and dental records, there is a fundamental difference of scale. Fingerprints are only useful if the tips of fingers are available, dental records are only useful if teeth are available. All that is required for profile matching is a miniscule trace of tissue, in saliva, hair roots and so on.

Nevertheless, we support the view that, for the purposes of the *Privacy Act*, genetic samples wiil only be reasonably identifiable to an individual if they are labelled or coded.

Question 7–4. Should genetic samples obtained in Australia be exported only to jurisdictions whose laws provide protections equivalent to that of the *Privacy Act* and the NHMRC's *National Statement* on Ethical Conduct in Research Involving Humans?

In our view it is vitally important that samples are only exported to countries with parallel provisions.

---

[9] R. Williamson and R. Duncan, 'DNA Testing for All' (2002) 418 *Nature* 585 have interestingly argued that the genetic profiles of *all* individuals should be collected at birth and stored, this would increase the likelihood that a particular piece of tissue could be re-identified.

Question 7–5. Is NPP 9 of the *Privacy Act* an appropriate model for regulating the export of genetic samples?

If genetic samples are included in the *Privacy Act* then NPP 9 should provide appropriate coverage.

Question 7–6. Does the *Privacy Act* adequately deal with issues that may arise in relation to the genetic samples and information of deceased individuals?

We believe that it is important for individuals other than the source of the genetic sample to be allowed access to the sample in certain limited circumstances. In particular, individuals other than the source should only be allowed access for health-related purposes and access should be limited to close relatives (parents, children and siblings). Specific provision may need to be made in the *Privacy Act* to provide for this.

Proposal 7–3. The *Privacy Act* should be amended to clarify that ‘health information’ includes genetic information, whether or not the information is collected in relation to the health of, or the provision of a health service to, an individual.

We agree with this Proposal.

Proposal 7–4. The *Privacy Act* should be amended to ensure that all small business operators that hold genetic information are subject to the provisions of the Act.

We agree with this Proposal.

With regard to the right not to know, we support the suggestion that a Temporary Public Interest Determination could be used to alleviate concerns about inappropriate disclosure under NPP 1.5.

(Attachment 3)

SUBMISSION

TO THE AUSTRALIAN HEALTH MINISTERS' ADVISORY COUNCIL

ON THE

NATIONAL HEALTH PRIVACY CODE (DRAFT) CONSULTATION PAPER

APRIL 2003

M OTLOWSKI AND D NICOL

CENTRE FOR LAW AND GENETICS

Submission authors

The authors are both members of staff in the Law Faculty at the University of Tasmania and members of the Centre for Law and Genetics. The Centre developed out of a project funded by the Australian Research Council from 1994-1997. The primary focus of the project was the ethical and legal implications of the 'new genetics'. Since then, the Centre has had further funding from the Australian Research Council and has expanded its areas of research to include broader issues associated with commercialisation of genetic technology.

The Centre examines legal standards in genetic technology, particularly in the following areas:

- collection, storage and banking of DNA (including DNA profiling);
- privacy of genetic information;
- discrimination in insurance and employment;
- patenting of biotechnological inventions;
- structuring of the biotechnology industry;
- domestic and international control of commercialisation of biotechnology; and
- regulation of stem cell research and cloning.

Associate Professor Otlowski lectures in Torts Law, Family Law, Employment Law and Health Law and Ethics. She is deputy Dirtector of the Centre for Law and Genetics and has expertise in the legal and ethical issues associated with human health and human genetic technology. Her particular research focus is on privacy and discrimination in relation to health and genetic information and she has published widely and presented talks on these issues.

Dr. Nicol lectures in Intellectual Property Law, Information Technology Law and Media Law and has developed expertise in privacy law in these areas. She also has expertise in the legal and ethical issues associated with human genetic technology. She coordinated the Hobart public consultation round of the Australian Law Reform Commission and Australian Health Ethics Committee inquiry on *Protection of Human Genetic Information* and made submissions on privacy related issues.

Introduction

In our view, the best option for comprehensively dealing with privacy in the healthcare context would be to have nationally consistent health privacy legislation. Nevertheless, the Draft National Health Privacy Code provides a useful statement of intent by state, territory and federal health ministers to be bound by a consistent set of rules for handling all health information. We do have some concerns about the reach of the Code and whether it can be truly 'national'. These concerns are discussed below under the heading 'Implementation'.

The special nature of health information and genetic information

We believe that, in drafting the National Health Privacy Code, Australian Health Ministers had the opportunity to debate and discuss the sensitive and complex nature of health information and craft privacy principles that pay due attention to these sensitivities and complexities. This has been achieved to a certain extent, particularly with regard to NHPP 1 and NHPP 6, but the NHPPs are really little more than a replication of the NPPs, relabelled to cover health. We would have liked to have seen more in depth consideration of the special nature of certain types of health information. We believe that genetic information warrants particular attention. The National Health Privacy Code includes genetic information in the definition of health information, when this is collected or used in connection with delivering a health service, or genetic information when this is predictive of an individual's health. We note that this provision mirrors the equivalent provision in the Privacy Commissioner's 2001 Guidelines on Privacy in the Private Health Sector (at 3.2). Whilst this provision does assist in determining that genetic information is health information in the clinical setting, it does not overly assist in determining whether genetic information used in the research context is health information. This is particularly problematic when genetic research is conducted by small businesses, which are exempt from the private sector obligations under the *Privacy Act* 1988 (Cth) unless they deal with health information.

We have a number of further concerns in relation to the definition of genetic information. Whilst the definition does extend to cover information that could be predictive of the health of an individual or his or her descendants, the definition of health service does not include diagnosis of carrier status or predictive testing.

The Final Report of the joint Australian Law Reform Commission/Australian Health Ethics Committee inquiry into *Protection of Human Genetic Information* is scheduled for release in May 2003. One of the proposals in the Inquiry's Discussion Paper was to extend the definition of personal information in the *Privacy Act* 1988 (Cth) to include human genetic samples. If this proposal is adopted in the Final Report and acted on by the Federal Parliament the definition of personal information in the Code would also need to be amended and the implications of the inclusion of genetic samples in relation to other provisions in the Code would need to be examined.

Other difficulties with genetic information

Genetic information has particular features that create troublesome issues in relation to information privacy. Perhaps the two most prominent features are the familial nature of genetic information and the capacity to re-identify the personal genetic information contained in a tissue sample after de-identification. We point to two specific issues that need to be addressed.

a. Disclosure of an individual's genetic information by their genetic relatives

NHPP1.1 (i) refers to information that is family, medical or social history. We query whether this includes genetic information collected from one person that is 'about' their genetic relatives. Perhaps this provision needs to deal with this issue in a more explicit manner.

This NHPP mirrors two Public Interest Determinations (PIDs) made by the Privacy Commissioner in October 2002 (PID 9 and 9A). The Commissioner has the power to reduce the privacy protection of any one or more of the NPPs through section 72 of the *Privacy Acy* 1988 (as amended). PIDs 9 and 9A allow for the collection of a third party's social, family or medical history where relevant to the provision of a health service to a consumer. Does this mean that an individual can disclose a relative's genetic test results without consent?

b. Access to an individual's genetic information by their genetic relatives

In Part 5 of the Code, clause 1 of Division 1 states that an individual has a right of access to all health information relating to the individual. The difficulty here is that genetic health information collected from one individual relates to their genetic family as well as themselves. Do all of these individuals have a right of access to information obtained as a result of the provision of a health service to one of them?

Clause 4 goes on to state that an individual may authorise the provision of access to others. Perhaps this could be an avenue for providing for the release of genetic information about an individual when it is provided by a genetically related individual.

NHPP1.7 deals with information given in confidence. We believe that this provision and NHPP 6.1 need to be explored in the context of genetic information. Genetic information could be provided in confidence by one person in relation to the provision of health services to them but could also relate to the provision of health services to their genetic relatives. If the person requests that the information not be communicated to any other individual to whom it relates, does the health service provider have to respect that request or are there circumsatnces when it could be overriden? Because there may be circumstances when failure to disclose could pose a serious threat to the life or health of an individual, in such circumstances it may be appropriate to override the obligation of confidence.

NHPP6.1 also deals with access to health information and also has relevant provisions relating to the issue of access to and disclosure of genetic information provided by one person but about them and their genetic relatives. Paragraph (b) allows for access to be refused when it would have unreasonable impact on the privacy of other individuals and paragraph (e) deals with information given in confidence. Again, in our view it is necessary to address the issue of when it may be appropriate to override these provisions. The Privacy Commissioner expressed the view in PIDs 9 and 9A that NPP6.1(c) (equivalent to NHPP6.1(b)) would control access to genetic information. He noted further that:

> 'The question of whether a health service should grant a request by a genetic relative for access to the genetic information is a matter of judgment for the service provider in the usual context of the professional obligation of patient condifentiality, and related professional training and guidance.'[10]

In our view, an issue of such sensitivity should not be left to individual service providers to determine on a case by case basis. It would be better to provide concrete guidance on this matter.

We note that Division 3 of the Code deals in some detail with NHPP6.1(a), where access to health information is refused on the ground that providing access would pose a serious threat to life or health of the individual. We are of the view that access to genetic information could be

---

[10] Public Interest Determination No. 9 at p.16.

similarly dealt with in Division 3 or in a new Division. There could be provisions that provide guidance on when to override a refusal by an individual to allow disclosure of their genetic information to genetic relatives, particularly when failure to disclose could pose a serious threat to the life or health of an individual.

c. The right not to know

Another concern about the inappropriate application of the privacy principles in the context of genetic test information relates to the protection of those individuals who choose not to know about genetic information relating to them.

The right of an individual not to know abut genetic information relating to them is supported in a number of international instruments[11] and plays an important role in relation to this form of predictive information. Significantly, it receives no special recognition under the *Privacy Act* or in the National Health Privacy Code. Not only is there no specific recognition or protection of the right not to know, there are provisions contained in the Act and the Code (in particular, NPP 1.5 and NHPP 1.5) which may encourage information to be inappropriately disclosed to the individual about whom it is collected in an over zealous attempt to comply with the requirements of the legislation.

It is vitally important that the right not to know is afforded appropriate protection under privacy legislation to ensure that the potential arising from the availability of genetic information does not become an unwanted burden.

Scope of the National Health Privacy Principles

Further to the submission made above, we strongly support the view that the National Health Privacy Code should cover the handling of all health information no matter where it is held. Our reason for this is that there are many instances where health information is required to be disclosed outside the health setting.

Implementation

One of the key objectives of this initiative to develop a National Health Privacy Code is to ‘achieve national consistency in health privacy protection – across jurisdictions and between the public and private sectors’ (National Health Privacy Code – Fact Sheet and Draft National Health Privacy Code, 2 Objects of the Code). From the outset, we wish to note that we strongly believe that there is a need for greater harmonisation in privacy laws in respect of health information across Australia. The present patchwork of coverage involves considerable duplication of effort between federal public and private sectors as well as state and territory legislation resulting in a situation which is complex and confusing, and where differences in coverage for example, between public and private sector regimes, are not always justifiable.

There is little, if any, explanation in the *National Health Privacy Code (Draft) Consultation Paper* or the accompanying Discussion Paper as to how this objective of full national coverage will be achieved although the Discussion Paper does note that options for implementation will be addressed by the Australian Health Ministers Council. It seems to us, however, that these as yet unresolved implementation issues have a direct bearing on the value of the Code, and whether indeed it can be described as a ‘national’ health privacy code.

---

[11] Council of Europe, *Bioethics Convention on Human Rights and Biomedicine,* Article 10; UNESCO, *Universal Declaration on the Human Genome and Human Rights,* Article 5.

From the information that can be gleaned from other sources, in particular, the ALRC/AHEC *Discussion Paper* 66 (2002) at para 7.31-7.32, it would appear that the National Health Privacy Code is expected to operate as a code under Part IIIAA of the *Privacy Act* 1988 (Cth). In particular, it is proposed that at the request of a state or territory government, regulations under the Act may prescribe an instrumentality of a state or territory as an 'organisation' for the purposes of the Act. This would provide a mechanism by which the operation of an approved code might be extended to the state and territory public sector health service providers.

Implementation of the National Health Privacy Code under Part IIIAA of the *Privacy Act* may be a sensible option, provided that it can be achieved and secure genuinally national coverage. If this is to be the approach adopted, it would appear that some significant obstacles remain to securing this objective. It may be difficult to make the Code mandatory, because of its cross-jurisdictional nature. In particular, it relies on the co-operation of all the States and Territories, some of which have already enacted their own privacy laws such as Victoria which has introduced specific health privacy legislation (*Health Records Act* 2001 (Vic)). As the ALRC/AHEC has already recognized (*Discussion Paper* 66 (2002) para 7.33), the enactment of State and Territory health privacy legislation 'may be seen as running counter to the proposal to develop a National Health Privacy Code to provide consistency across all jurisdictions'. Furthermore, doubts were expressed as to whether the Australian Health Ministers' Advisory Council process will lead to uniformity or greater harmonization of health privacy law in the short term. We share these concerns.

Moreover, this approach to implementation does not cover private sector organisations which presumably would continue to be bound by the NPPs in the *Privacy Act* 1988 (Cth). To the extent of any variation between the NPPs and NHPPs, the goal of uniformity will be undermined. Even more significantly, it detracts considerably from the idea of a national code on health privacy that applies uniformly to all if a large component of the population is subject to another regime, albeit containing the same key principles, in this case, embedded within the general NPPs. The concept of a 'National Health Privacy Code' creates an expectation that there will be uniform coverage of a single set of principles specifically focused on health privacy. Whilst the final outcome might be much the same (requirements of NHPPs together with coverage of health information within the NPPs) it seems to us a little misleading to describe as a 'National Health Privacy Code' what really amount to a sharing of principles across public and private sectors.

One option for maximising coverage of the National Health Privacy Code (accepting that it is unlikely that the National Health Privacy Code can be made mandatory for private sector organisations), is to encourage private sector organisations to comply with the more specific NHPPs. Perhaps the best way to encourage compliance would be to have a list of service providers who have opted in and to allow these organisations to use a badge indicating compliance with the Code as demonstrating 'best practice'.

We emphasise our concern that some gaps in coverage may still remain, for example, small businesses that are not providing a health service (eg genomics companies) may not be obliged to comply with the NPPs.

Enforcement Issues

No information is provided in the *National Health Privacy Code (Draft) Consultation Paper* about mechanisms for enforcement of the proposed National Health Privacy Code and how non-compliance is to be dealt with. If the National Health Privacy Code is implemented through the mechanisms available under Part IIIAA of the *Privacy Act* 1988 (Cth) (as amended) and consequently shares the same enforcement regime as that legislation, it will be open to some of the same criticisms that have been levelled at the new private sector *Privacy Act* amendments.

The privacy regime is complaints-driven and conciliation-based. Orders of the Privacy Commissioner can only be enforced by court action. Thus, one of the major drawbacks of the proposed National Health Privacy Code is that this is ‘soft touch’ legislation and enforcement powers are relatively weak when compared with common law actions. This may lead to a situation where the National Health Privacy Code gives the impression of being effective and enforceable, couched as it is in mandatory language, yet in reality lacks an effective enforcement mechanism. However, we do recognise that there are many advantages of conciliation over litigation.

(Attachment 4)

The following is a copy of the manuscript that was published in the Australian Journal of Labour Law:
'(2001) 14 *Australian Journal of Labour Law* 169-176

'Employment Sector By-Passed by the Privacy Amendments'

by Margaret Otlowski

Introduction

Late last year the Commonwealth Parliament passed legislation introducing a national scheme of privacy regulation to the private sector. The *Privacy Amendments (Private Sector) Act* 2000 (Cth) received Royal Assent on 21 December 2000 but will not come into force for 12 months from that date. (Section 1 of the *Privacy Amendments (Private Sector) Act* 2000 (Cth) provides that the Act will come into effect on 1 July 2001 or 12 months after it received Royal Assent whichever is the later.) However, despite the otherwise wide-ranging nature of this legislation, it has been specifically framed to confer on employers an exemption from compliance with the new National Privacy Principles in respect of employee records. The purpose of this note is to explore and critique the basis for that exemption.

Background

A system of privacy protection in the public sector has been in place in Australia for quite a number of years. The *Privacy Act* 1988 (Cth) contains a series of Information Privacy Principles which stipulate that information about individuals is to be collected fairly, lawfully, and with the knowledge and consent of the individual from whom it is collected, (Information Privacy Principles 1, 2 and 3) and which prohibit collection of information unnecessarily or for an unlawful purpose (Information Privacy Principle 1). The principles also regulate the storage of information (Information Privacy Principle 4). and require that records are up-to-date (Information Privacy Principle 7). Further, the principles limit the use and disclosure of personal information held by an agency (Information Privacy Principles 10 and 11). However the operation of this legislation has been limited to Commonwealth government departments or agencies and for many years, concerns had been expressed about the adequacy of protection for information held by non-Commonwealth organisations in the private sphere. (See, for example, Privacy Commissioner, first Annual Report on the Operation of the *Privacy Act* 1988 (Cth); House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence. A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth.* June 1995.) Concerns had also been raised about the inadequacy of sanctions for improper disclosure (*In Confidence* Report (above) at 31).

Introduction of Privacy Reforms to the Private Sector

In response to growing calls for privacy regulation in the private sector, and the apparent unwillingness of the Coalition Government to legislate (despite an earlier election commitment to act on this issue), in February 1998 the Federal Privacy Commissioner issued National Principles for the Fair Handling of Personal Information (Office of the Federal Privacy Commissioner, 'National Principles for the Fair Handling of Personal Information' (1998)). These principles regulating the collection, storage, use and disclose of personal information, were developed for business after consultation with representatives from various industries as well as a wide range of consumer and government representatives.

When the Government did finally move to legislate with the introduction of the *Privacy Amendment Bill* 1998 (Cth), the scope of the legislation was limited to personal information held by contractors in relation to services provided to the Commonwealth. This Bill was referred to the Senate Legal and Constitutional References Committee which took the view that wider ranging privacy protection was necessary and recommended that the Government introduce legislation to provide privacy protection uniformly covering the public, private, charitable and 'not for profit' sectors (Senate Legal and Constitutional References Committee, *Privacy and the Private Sector: Inquiry into Privacy Issues, including the Privacy Amendment Bill 1998* (1999) Recommendation 4). It was recommended that the coverage of the legislation should be as broad as possible and the extent of any exemptions should be kept to a minimum. With particular reference to the employment sector, the Senate Legal and Constitutional References Committee expressed concerns about the proposed exclusion of employee data from the scope of legislative privacy protection, but noted claims of employer groups that existing legislation provided adequate coverage. It was accordingly recommended that in the development of more effective privacy legislation, consideration be given to the relationship between existing laws regulating employer records and proposed legislation which would seek to cover employee data (Senate Legal and Constitutional References Committee, (above) para. 3.22).

The Government's response to calls for wider ranging privacy protection was in the form of the *Privacy Amendments (Private Sector) Bill* 2000 (Cth) which has since been passed establishing a comprehensive national scheme for the protection of personal information by the private sector. The effect of this legislation is to create new National Privacy Principles for the private sector, expanding on the National Principles for the Fair Handling of Personal Information issued earlier by the Federal Privacy Commissioner. It applies to 'organisations' defined in section 6C as meaning an individual, or a body corporate, or a partnership, or any other unincorporated association, or a trust that is not a small business operator, a registered political party, an agency, a State or territory authority or a prescribed instrumentality of a State or Territory ('small business' is in turn defined in s 6D as a business with an annual turnover of $3 million or less.) The new provisions apply to 'personal information' which is defined in s 6(1) of the *Privacy Act* 1988 (Cth) as meaning 'information or an opinion, … whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information.'

The legislative approach is one of 'co-regulation' or so called 'light-touch.' According to the Explanatory Memorandum accompanying the Bill, the term 'co-regulation' refers to a legislative framework within which self-regulatory codes of practice can be given official recognition. Legislation will establish the general principles and minimum benchmarks or safeguards with which all private organisations must comply and organisations and industries will be encouraged to develop codes of practice, using the National Privacy Principles as a benchmark, which are then to be approved by the Privacy Commissioner. (*Privacy Amendment (Private Sector) Bill 2000, Explanatory Memorandum*, 12.) In the absence of an industry code, the National Privacy Principles apply by way of default position requiring organisations to comply with the guidelines for the collection, holding, use, disclosure and transfer of personal information.

The Employee Records Exemption

A notable feature of the legislation is the wide exemption it contains for employee records in s 7B(3). The term 'employee record' is defined broadly in s 6(1) of the *Privacy Act* 1988 (Cth) (as amended by the *Privacy Amendment (Private Sector) Act* 2000 (Cth)) as a record of personal information relating to the employment of an employee. The section goes on to give as examples of personal information relating to the employment of the employee, health information about the employee and personal information about all of any of the following: a) the engagement, training, disciplining or resignation of the employee; (b) the termination of the employment of the employee; (c) the terms and condition of employment of the employee; (d) the employee's personal and emergency contact details; (e) the employee's performance or conduct; (f) the employee's hours of employment; (g) the employee's salary or wages; (h) the employee's membership of a professional or trade association; (i) the employee's trade union membership; (j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave, (k) the employee's taxation, banking or superannuation affairs.

The exemption is framed in such a way that it will only apply to acts or practices 'directly related' to an 'employee record' and a current or former employment relationship. (See s 7B(3) which states that employee records will be exempt from the operation of the legislation if the organisation is or has been an employer of the individual in question and the act or practice is directly related to i) a current or former employment relationship between the employer and the individuals <u>and</u> ii) an 'employee record' held by the organisation and relating to the individual.) Thus, it would not protect an employer who purports to collect, use or disclose information about an employee for purposes *unrelated* to that relationship. These dual requirements (current or former employment relationship and an employee record) are intended to ensure that employers do not take commercial advantage of the exemption. According to the proponents of the legislation, an employer, would, for example, be precluded from selling information contained in an employee record to a direct marketer as such conduct would fall outside the scope of the exemption: Attorney General, The Honourable Mr Williams MHR, Second Reading Speech, 12 April 2000, House of Representatives, *Hansard* p 15077. Moreover, the exemption is limited to existing or former employees so would not apply to information provided in confidence to an employer by a prospective employee: individuals in those circumstances would be able to assert that the employer is bound to comply with the new National Privacy Principles (See Office of the Federal Privacy Commissioner, *Fact Sheet 5 – Exemptions* (2001)). This is because the exemption only comes into play if and when the person becomes an employee, in which case, it applies to all personal information gathered by the employer in relation to that person including information gathered in connection with recruitment. Guidelines are being prepared by the Office of the Privacy Commissioner to further clarify the meaning of the employee records exemption and its precise scope.

The employee records exemption has been justified on the basis that whilst this type of personal information is deserving of privacy protection, such protection is more properly a matter for workplace relations legislation and has therefore been expressly excluded from the expanded privacy legislation. (Attorney General, The Honourable Mr Williams MHR, Second Reading Speech, 12 April 2000, House of Representatives, *Hansard* p 15077.)

Reviews by Commonwealth Parliamentary Committee of the Employee Records Exemption and the Government's Response.

The exemption for employee records was one of the matters canvassed by the House of Representative, Standing Committee on Legal and Constitutional Affairs after the *Privacy Amendments (Private Sector) Bill* 2000 (Cth) was referred to it for inquiry and report. The majority of the submissions to the committee touching on this issue echoed the concerns voiced earlier by the Senate Legal and Constitutional References Committee. Submissions from the ACTU, the Federal Privacy Commissioner, the Australian Privacy Charter Council, the Communications Law Centre and others strongly opposed the exemption and urged the Committee to recommend its deletion. In its Report, the Committee concluded that it was not satisfied that existing workplace legislation provides enough protection for the privacy of private sector and made clear its grave concerns about the proposed exemption (House of Representative Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill* 2000 (2000) para 3.29). In the Committee's opinion, the need for privacy protection is particularly evident having regard to the information which may be held by employers, including extremely sensitive health information such as genetic test results (para 3.30). The Committee was concerned that as a consequence of this exemption, there was potential for disclosure of such information without the employee's consent (para 3.32). Such disclosure could have a profoundly negative effect on the employee's life and may relate to information which a potential future employer may not, in any event, legitimately have the right to seek (para 3.32). The Committee was of the view that, given employees have little choice about providing such information to their employers, they are entitled to expect that their trust will be respected and the necessary confidentiality of their records ensured (para 3.33).

The Committee acknowledged that there is a difference between health, family or financial information on the one hand, and information relating to disciplinary matters or career progression on the other. In the Committee's view, the former was inappropriate for inclusion in the exemption and should not be released to others except with the employee's consent. Particular reference was made to the need to remove 'health information' from the definition of 'employee record': the view was vigorously expressed that given the nature of much health information, it is inappropriate for inclusion in such an exemption and inconsistent with the more specific protection given to health information and sensitive information elsewhere in the Bill (para 3.37).

It was recommended that most information contained in 'employee records' be given the protection of the National Privacy Principles. It was accordingly recommended that rather than spelling out the matters exempt from privacy exemption, the definition of 'employee record' be revised to specify personal information in relation to employment which would be protected. To this end, it was suggested that matters relating to engagement, training, disciplining or resignation of the employee, termination, and performance or conduct should be removed from the definition because these were very much work-related issues which ought to be exempt from privacy protection. The modified definition of employee records recommended by the Committee and intended to be subject to privacy protection was as follows (Recommendation 5):

> 'employee record,' in relation to an employee, means a record of personal information relating to the employment of the employee *other than an exempt employee record*. Examples of personal information relating to the

employment of the employee are health information about the employee and personal information about all or any of the following:

(a) the terms and conditions of employment of the employee;
(b) the employee's personal and emergency contact details;
(c) the employee's hours of employment;
(d) the employee's salary or wages;
(e) the employee's membership of a professional or trade association;
(f) the employee's trade union membership;
(g) the employee's recreation, long service, sick, personal maternity, paternity or other leave;
(h) the employee's taxation, banking or superannuation affairs. (changes from the Bill as initially proposed in italics.)

Excluded from the list of personal information in the Bill were paragraphs (a) the engagement, training, disciplining or resignation of the employee; (b) the termination of the employment of the employee and (e) the employee's performance or conduct: which, in the opinion of the Standing Committee were the only matters that ought to be covered in the exemption.

The Committee thought it appropriate to target more narrowly the information to which the exemption should apply, in place of the very broad exemption proposed under the Bill for 'employee records', widely defined. The Committee (Recommendation 6) was of the opinion that the exemption should be limited to records in relation to:

(a) the engagement, training, disciplining or resignation of the employee;
(b) the termination of the employment of the employee;
(c) the employee's performance or conduct.

Recommendations for a new definition of 'exempt employee record' in these terms were accordingly made. To give effect to this recommendation it was proposed that the provisions conferring an exemption on employers from compliance with the National Privacy Principles only apply in respect of exempt employee records as defined (Recommendation 7).

These recommendations were, however, rejected by the Government in its official response to the House of Representative, Standing Committee's report (Commonwealth of Australia, *Government Response, House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000,* September 2000). The decision not to accept the recommendations was justified on the grounds that State and Territory legislation already exists and that intervention by the Commonwealth Government in this area may be counterproductive:

> The regulation of employee records is an area that intersects with a number of State and Territory laws on workplace relations, minimum employment conditions, workers' compensation and occupational health and safety, some of which already include provisions protecting the privacy of employee records. The Government considers that the attempt to deal with employee records in the Bill might result in an unacceptable level of interference with those State and Territory laws and a confusing mosaic of obligations. (p 4)

The Standing Committee's recommended changes were therefore ignored in the final form of the legislation that ultimately was passed by the House of Representatives: the employee records exemption provision appearing in the same terms as in the original Bill. However, this approach to the issue is unsatisfactory. As noted earlier, there are some statutory protections applying to the public sector (*Privacy Act* 1988 (Cth) and the *Freedom of Information Act* 1982 (Cth)) but for the majority of workers in Australia there is little tangible protection of the privacy of their employment records. Whilst the *Workplace Relations Act* 1996 (Cth) makes some provision in relation to the maintaining of records (see s 353A and Part 9A of the *Workplace Relations Regulations*) this is aimed at ensuring that certain specified employment information is documented and available for official inspection for auditing purposes. (See *Workplace Relations Regulations* reg 131D. Note also regs 131E-131J.) Employees do have a right to have a copy of this record (*Workplace Relations Regulations* reg 131L) and to have errors in the record corrected (*Workplace Relations Regulations* reg 131K) but the primary purpose of these provisions is not protection of employee privacy. Moreover, privacy protection is not an allowable matter for the purposes of s 89A(2) of the *Workplace Relations Act* 1996 (Cth). Thus, privacy is not a matter which the Industrial Relations Commission has jurisdiction to make an award. At the State level, legislation only imposes very basic obligations in relation to the keeping of employment records: as at the Commonwealth level, the primary purpose of this legislation is to ensure documentation of key employment information rather than privacy protection. (*Industrial Relations Act* 1996 (NSW) s 129; *Industrial Relations Act* 1999 (Qld) Ch 11 Pt 1, *Industrial and Employee Relations Act* 1994 (SA) s 102, *Minimum Conditions of Employment Act* 1993 (WA) Pt 6; *Industrial Relations Act* 1984 (Tas) s 75.) Thus, the current coverage of employee privacy in the workplace relations context is minimal and patently inadequate as was recognised by the House of Representatives, Standing Committee on Legal and Constitutional Affairs. (House of Representative Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill* 2000 (2000) paras 3.7 and 3.29.)

The protection available through the ordinary courts is also far from satisfactory. There are existing contractual and equitable principles for maintaining confidentiality which may offer some protection to employees. (See B. Creighton and A. Stewart, *Labour Law: An Introduction* (2000) Federation Press p 256- 257 regarding possible contractual remedies and for reference to relevant equitable principles see *Smith Kine and French Laboratories (Aust)* v *Secretary, Department of Community Services and Health* (1990) 22 FCR 72, 92 and 95-98). However, such actions are, in practice, costly to pursue (involving private litigation in the civil courts) and not easy to establish. In short, neither existing legislation in the workplace context nor common law or equitable principles provide adequate protection of the privacy interests of employees, pointing to a clear need for the new National Privacy Principles to apply in the employment sector. Inclusion of the broad exemption in the legislation for employee records consequently leaves employees vulnerable to breaches of privacy at the hands of their employers, in respect of which they would not necessarily have a remedy. Ironically, because the exemption is limited to current or former employees, prospective employees are currently in a better position in terms of the protection of their confidential information than are persons who are or have been employees.

The employee records exemption was also considered by the Senate Legal and Constitutional Legislation Committee before the final passage of the privacy amendments *(Senate Legal and Constitutional legislation Committee, Consideration of legislation referred to the Committee: Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* October 2000). The Senate Committee noted that whilst there was support for the exemption from some quarters, for example, the Australian Chamber of Commerce and Industry, it also noted considerable opposition to it. Particular reference was made to the submission of the Privacy Commissioner which had argued that if the Government's objective in exempting employee records is to ensure that only one piece of legislation applies to protect this information, there is a need for a detailed analysis of the adequacy of the law that currently applies to protect the personal information about employees held by employers. To this end, the Privacy Commissioner had suggested that the employee exemption be subject to a 'sunset' clause of one year. The substance of suggestion was adopted by the Senate Legal and Constitutional Legislation Committee. It recommended that a sunset clause be included in the Bill to allow the exemption to operate for two years while analysis is undertaken by relevant agencies to ascertain whether existing workplace relations and State and Territory legislation is adequate to protect the privacy of employee records (para 3.21).

Ultimately, however, the Government decided against a sunset clause which would operate to automatically terminate the exemption at the end of the specified period. Instead, it announced that it will review existing Commonwealth, State and Territory laws to consider the extent of the privacy protection from employee records and whether there is a need for further measures (Joint News Release by the Commonwealth Attorney General Daryl Williams and Peter Reith, Minister for Employment, Workplace Relations and Small Business 29 November 2000). This review, to commence before the privacy amendments come into effect, is to be carried out by officers of the Attorney General's Department and the Department of Employment, Workplace Relations and Small Business and is to involve consultation with State and Territory Governments, the Privacy Commissioner and other key stakeholders. It is to be completed in time to assist the Privacy Commissioner when he conducts the more general review of the legislation two years after it commences operation.

Conclusion

National privacy legislation for the private sector has been a long time coming. It is a matter for regret that legislators chose to overlook the valid concerns raised by the Senate Legal and Constitutional References Committee and the House of Representatives Standing Committee on Legal and Constitutional Affairs regarding the employee records exemption and instead, rely on dubious grounds to justify the broad terms of the exemption. As a result, an important opportunity has been missed to include the employment sector within the new national scheme of privacy regulation and extend to employees legislative rights to privacy protection. Even the more watered down protection recommended by the Senate Legal and Constitutional Legalisation Committee allowing the exemption subject to a two year sunset clause would have been a preferable outcome: although the Government has promised that a review be undertaken of the adequacy of existing privacy protection for employee records under Commonwealth, State and Territory legislation, there is no guarantee that this will result in strengthened privacy protection in the employment sector.