SUBMISSION TO THE

AUSTRALIAN LAW REFORM COMMISSION

REVIEW OF PRIVACY IN RESPONSE TO

***DISCUSSION PAPER* 72**

FROM

PROFESSOR MARGARET OTLOWSKI

PROFESSOR DONALD CHALMERS

AND

ASSOCIATE PROFESSOR DIANNE NICOL

ON BEHALF OF THE

CENTRE FOR LAW AND GENETICS

DECEMBER 2007

Introductory Comments: explanation of approach to our submission

This submission on behalf of the Centre for Law and Genetics (CLG) deals somewhat selectively with the issues raised in this *Discussion Paper*. In particular, it seeks to respond to the proposals and questions in the *Discussion Paper* which concern a consistent and unified national framework for privacy regulation in Australia and the privacy regulation of health information. The submission also addresses a few other areas where we have the knowledge and expertise to provide comment. Where we have no comment on specific proposals or questions, we have simply deleted the proposals and question from our submission.

In the opening section of this submission we wish to address what we see as the key framework for the privacy reforms proposed, in particular, the *Discussion Paper's* proposals for achieving national consistency and for restructuring and unifying the *Privacy Act* 1988 (Cth) and the principles that it contains.

Introduction to the Inquiry (Chapter 1, Proposal 1-1)

The CLG supports this Proposal as it recognises the unique cultural contexts of privacy for particular indigenous and other ethnic groups. In addition, by placing responsibility for the development of these protocols with the Office of the Privacy Commissioner (OPC) (or, if Proposal 43-1 is accepted, the Australian Privacy Commissioner or APC), there is consistency within the framework of the *Privacy Act 1988* (Cth) to establish general principles which can be operationalised in specific contexts.

The *Privacy Act* (Chapter 3, Proposals 3-1 to 3-13)

The CLG strongly supports the structure in Proposal 3-1 of Unified Privacy Principles (UPPs) operationalised to particular contexts by regulations. This structure will enable the development of national and consistent approaches to privacy in the health area, in particular, with the development of Privacy (Health Information) Regulations.

Importantly, there is a need for consistency between national regulations and the rapidly developing e-health environment. E-health will extend beyond national borders and will require consistency with North American and European regulations. The proposed framework of general UPPs and subsidiary contextual regulations will also promote this international consistency.

We strongly support Proposals to develop a consolidated single set of UPPs and to simplify and clarify the current legislation, which is complex, labaraynthine and not comprehensive. We also support the inclusion of the objects clause (Proposal 3-4).

While the CLG supports the development of a statutory cause of action for invasion of privacy (see our submission in relation to Chapter 5) we doubt the value of including

the action in the *Privacy Act 1988* (Cth) (for reasons set out below). We support the proposed change in title to *Privacy and Personal Information Act.*

With regard to the definition of personal information and sensitive information, we note that ALRC 96 Recommendations 7.4 and 8.2 proposed that health information was to be redefined in the current *Privacy Act* to include genetic information and similarly, genetic samples. Whilst the recommendation to expressly include genetic information within the definition of health information has been implemented through amendments to the Privacy Act (*Privacy Legislation Amendment Act 2006* (Cth)), the recommendations to protect the privacy of genetic samples have not been acted upon. This recommendation should be revisited and considered for inclusion in the final report.

The CLG continues its support for privacy protection of personal information of individuals who have been dead for up to 30 years (Proposal 3-11). In addition Proposal 3-12 is supported as it is consistent with the general approach in the proposed section 95AA rules that are currently under development.

National Consistency (Chapter 4, Proposals 4-1to 4-7)

We reiterate our view, as stated in the submission in response to the *Issues Paper,* that national consistency in the regulation of personal information is indeed important and should be one of the key objectives of any privacy reforms for Australia. National consistency will also enable the development of consistency with emerging international privacy standards (for example, as the *Discussion Paper* mentions, the NPPs were influenced by the EU Directive on Data Protection). National consistency is also an essential response to the nationalising and internationalising of business, credit, banking and health services. Significantly, this has been the unanimous view of the Senate Committee inquiry into privacy and the Review undertaken by the OPC.

We had indicted in our earlier response our preference for comprehensive national legislation or some form of complementary scheme provided that consistency could be assured. We are of the view that the proposals contained in this chapter setting out a Commonwealth-state cooperative scheme strike the right balance, unequivocally indicating the intention to cover the field with regard to the privacy regulation of personal information by organisations in the private sector. Given the proposals for corresponding amendment of state and territory legislation (Proposal 4-2), and for applying minimum coverage based on the revised federal principles (proposed UPPs) to the state and territory's public sector (Proposal 4-4), we strongly support the proposal for review after 5 years to evaluate whether this Commonwealth-state cooperative scheme has been effective in achieving the desired national consistency (Proposal 4-5). We also strongly endorse the proposed strategies for promoting and maintaining uniformity (Proposal 4-6).

We are of the view that implementation of these proposals would alleviate much of the current complexity stemming from the current fragmentation including the potential for overlap of regulation, such that a single piece of personal information may be subject to more that one legislative regime at the same time. In so doing, these

reforms will reduce the compliance burden and associated cost for organisations and facilitate the appropriate sharing of information between sectors.

As we had indicated in our earlier submission, the goal of national consistency in the operation of privacy principles should not preclude targeting particular areas that warrant special treatment, such as health privacy. We respond to the *Discussion Paper's* specific proposals in respect of the regulation of health privacy below, but note for present purposes, that we support the broad thrust of those proposals which seek to maximise achieving consistency of the revised federal principles (proposed UPPs) but at the same time, acknowledging the special considerations pertaining to the health area. We believe that this will adequately cater for the practical needs of this complex area without detracting from a coherent national privacy scheme in Australia.

Protection of a Right to Personal Privacy (Chapter 5, Proposals 5-1-5-7)

We are very pleased to see that the ALRC has proposed a statutory cause of action for invasion of privacy. In our view it is entirely appropriate that such a cause of action should be enshrined in legislation. While some incremental developments are being made by the courts in this regard, progress is slow and outcomes for litigants are far from certain. If the Australian courts were to develop the cause of action under the guise of breach of confidence, following UK precedents, then protection would be limited, encompassing only the public disclosure of private facts. Other aspects of invasion of privacy, as itemised by the NSWLRC and set out in more limited form in Proposal 5-1, should also be included. Interference with an individual's home and family life is equally as invasive as public disclosure of private facts.

We also support the proposals by the ALRC that the appropriate tests should be reasonable expectation of privacy and sufficiently serious act to cause substantial offence to a person of ordinary sensibilities. In our view these tests accord with international best practice.

However, we do have some concerns with the proposal that the statutory cause of action should be included in the *Privacy Act 1988* (Cth). First, the Act deals with information privacy and the proposed statutory case of action is much broader. Placing the statutory action in this legislation may diminish its importance and potential scope. Secondly, the structure of the Act is to establish general principles that are operationalised in specific contexts by guidelines from the OPC/APC. This may not fit well with the statutory litigation model of the proposed cause of action. Thirdly, the conceptual framework of the Act is about obligations of information holders and the promotion of best practices. This can be enforced by a statutory complaints mechanism that does not necessarily require a full statutory right to privacy. Finally, the addition of yet another component to an already complex piece of legislation may cause confusion rather than clarify rights and obligations.

We also have some concern about the defence mooted in part (c) of Proposal 5-5. In its present format, the defence limits the circumstances in which public interest can be raised to disclosures of information. In our view there may be other circumstances in

which public interest can be raised even though there has been no disclosure of information and there is no intention to disclose information. Such circumstances could arise in relation to the types of invasion of privacy listed in parts (a) and (b) of Proposal 5-1.

The Costs of Inconsistency and Fragmentation (Chapter 11 Proposal 11-1)

This Proposal recognises that the protection of privacy must be balanced against the need to share personal information with other organisations for valid reasons. Privacy must not promote a culture of secrecy, particularly as e-health develops with a capacity for beneficial transmission of personal health information. This Proposal will hopefully promote information sharing in a responsible, ethical and professional fashion within the overriding UPPs and developed contextual rules.

Structural Reform of the Privacy Principles (Chapter 15 Proposals 15-1-15-4)

We had made clear in our earlier response to the *Issues Paper,* our concerns about unnecessary complexity of having different parallel regimes for the public and private sector (Information Privacy Principles (IPPs) alongside the National Privacy Principles (NPPs)) and our support for rationalisation of these principles in a more unified form applicable across public and private sectors. Accordingly, we strongly endorse the proposals contained in the *Discussion Paper* for structural reform of the privacy principles through the development of UPPs through consolidation of the existing IPPs and the NPPs (Proposals 15-2). We also support the proposal for the NPPs to be used as the template in drafting and restructuring the proposed UPPs (Proposals 15-4): these principles, which are derived from the OECD Guidelines, are of more recent origin and have been influenced by international requirements. As such, they are a useful template for the planned consolidation process. We noted in our earlier submission, these principles have also been influential in the development of principles for privacy legislation in Victoria, Tasmania and the Northern Territory. Moreover, as the NPPs were developed for the private sector taking account of compliance capacity, adopting these as the template would keep to a minimum the compliance burden and costs of such a change for Australia as a whole. We acknowledge the need to modify the application of the unified principles for particular sectors (eg health), but as a matter of principle, we are strongly in support of a more homogenous and uniform approach to privacy regulation in Australia.

Unification of federal privacy law, through the development of a unified set of principles, together with the proposals noted above for achieving national consistency, represent crucial steps for addressing the many problems of inconsistency (for example in the treatment of ‘sensitive information’ as between private and public sectors) and other unnecessary complexities which currently pervade this area.

Further to the above, we also support the goal of the obligations in the privacy principles being expressed as 'high level' principles (ie the concept of high-level 'guidance', supported by Codes of Practice), which are accessible (simple, clear and easy to understand) and which impose reasonable obligations on agencies and organisations (Proposal 15-1).

Consent (Chapter 16, Proposal 16-1)

We note that the development of biobanks for health research will require the development of specific governance and ethical rules relating to consent, particularly for future (possibly unspecified) research. The NHMRC is developing policies but the rules should be ratified, if not prepared, by the OPC/APC, in the public interest. In addition, these rules will have to be internationally consistent. These rules should also be consistent with the current consent provisions in the *National Statement on Ethical Conduct in Human Research.*

Specific Notification (Chapter 20, Proposals 20-1 to 20-7)

The CLG strongly supports the need for specific notification. There is a public perception that organisations and agencies collect information without any notification. These Proposals address this concern and reasserts the general principle that information should only be collected, stored and used for a specific legitimate purpose. This principle can then be operationalised with OPC/APC guidance for specific purposes.

Use and Disclosure (Chapter 22 Proposals 22-1 to 22-3)

The CLG agrees with the proposal that a new 'use and disclosure' principle should be included in the proposed set of UPPs. The CLG also agrees that the proposed 'use and disclosure' principle should contain an exception permitting an agency or organisation to use or disclose information for:

a. a secondary purpose related to the primary purpose of collection; and
b. where an individual would 'reasonably expect the agency or organisation to use or disclose the information for the secondary purpose'.

No doubt the ALRC Inquiry has received many submissions and other representations on the difficulties encountered by agencies in obtaining information on the basis of concerns about privacy. This exception recognises two important qualifications, namely, secondary purposes closely related to the primary purpose and a 'reasonable expectation' test. This UPP can be operationalised by guidelines prepared by the OPC/APC. The CLG also notes that the UPP of openness (Proposal 21-1) requires agencies not organisations to openly and transparently notify how information is collected, held, used and disclosed by them. This openness principle should also require these agencies and organisations to post on their websites, from time to time,

notification of general agency and organisational uses of information for 'secondary purposes' or under the reasonable expectation exception. This proposal is intended to facilitate, rather than inhibit, the proper use of information for the benefit of the individual (or in the case of research, for public interest). There should be 'a reasonable expectation' under the openness UPP that agencies and organisations notify through their website any changes in the disclosure of information for secondary and reasonable expectation purposes.

Data Security (Chapter 25, Proposals 25-1 to 25-6)

The CLG supports the introduction of a UPP on 'data security' and also the development of guidelines from the OPC/APC on the meaning of 'reasonable steps' to be undertaken by an organisation that releases information under a contract, encryption standards and staff training. This unified principle recognises the continuing responsibilities of agencies and organisations for the information they hold. The CLG also agrees with the proposal (25-5) that the OPC/APC develop guidance on when it is appropriate to destroy or render non-identifiable information no longer needed for a purpose permitted under the UPPs. The CLG notes however, that the destruction or rendering non-identifiable guidance must recognise the unique requirements of the health and research environments. The *Australian Code for the Responsible Conduct of Research* lays down a minimum of a 5-year period for the retention of data for purposes of verification and authentication. Similarly, in clinical trials, data should be retained for follow-up and verification purposes. In the case of genetic information, specific guidance may be required with regard to the use of such information for longitudinal epigenetic research purposes. The unique nature of genetic information has been recognised in ALRC Report 96.

Transborder Data Flows (Chapter 28, Proposals 28-1 to 28-10)

The CLG strongly supports the inclusion of a unified privacy principle on 'transborder data flows'. This UPP recognises the globalisation of information exchange, the potential for e-health outside of Australian borders and international requirements for transborder data flow (particularly the EU requirements).

The development of international standards will be promoted by Proposal 28-4, requiring agencies and organisations to consider, if not require, checks on the stands of privacy protection in the jurisdiction in which they intend to transfer information.

Employee Records Exemption (Chapter 36, Proposals 36-1 and 36-2)

The CLG supports the proposal to remove the current exemption for employee records. The CLG notes the modern development of best practice in relation to openness and access of employees to employer records. However, this development is not uniform as yet. Accordingly, we believe that it is appropriate to include an

exception allowing agencies or organisations to deny access to evaluative material (Proposal 36-2).

Structure of the Office of the Privacy Commissioner (Chapter 43, Proposals 43-1 to 43-5)

We support the change of name from Office of the Privacy Commissioner to the Australian Privacy Commission. This reflects the expanded functions of the Privacy Commissioner, the delegation of functions to deputies and the expanding and increasing importance of privacy in the computer and internet age.

Regulatory Framework for Health Information (Chapter 56, Proposals 56-1 to 56-5)

Within the context of a composite package for reform of privacy in Australia, as proposed in the *Discussion Paper,* we are content to endorse the proposals contained in this chapter for the regulation of health information. In particular, we note other key proposals addressed above, for achieving a nationally consistent framework, based on unified privacy principles. Against this background, we accept the merit of the proposals under which health information would continue to be regulated by the general provisions of the *Privacy Act,* pursuant to the revised UPPs, but amended as appropriate for the health information context by the proposed *Privacy (Health Information) Regulations* (Proposal 56-1). This would achieve the goal of a single, national set of principles applying to the health and non-health information rather than two sets of principles: one dealing with health information and one dealing with other personal information, which would be especially problematic for organisations dealing with both categories of information. It will also means that the UPPs are kept as simple and concise as possible in terms of their general application.

In our earlier submission in response to the *Issues Paper,* we had indicated as our preferred position, that there should be a separate set of privacy principles for the regulation of health information to those used to regulate other sensitive personal information. We had put this forward on the basis of the highly sensitive and complex nature of health information, which includes different types of information within it, including the particularly sensitive area of genetic information which is not only very personal information, but also has a shared, familial dimension. We expressed the view that enacting a separate set of privacy principles dedicated to health information would allow the privacy standards to accommodate the particular characteristics and the sensitive nature of health information in general. Further, it would allow scope for developing particular provisions within that set of principles recognising the special nature of certain types of health information such as genetic information. We had given in principle support to the draft *National Health Privacy Code,* ideally implemented by way of national health privacy legislation, with a view to maximising visibility and ensuring ongoing uniformity of coverage.

We believe, however, that the compromise approach which is proposed in chapter 56 does, to a considerable extent, address our concerns about the need to be able to cater for the unique and challenging demands of the health care sector through the

modification of the UPPs via the *Privacy (Health Information) Regulations*. Importantly, we note the recognition in the *Discussion Paper* (para 56.73) that handling health information does raise some unique issues and that these require additional consideration in the development of privacy principles, rules and guidelines. Further, we believe some of the features of the current regime which exacerbate the problem of inadequate coverage in the health sector will be addressed if the proposed reforms are implemented, namely fragmentation between the NPPs and the IPPs, and the growth of state and territory legislation also seeking to regulate this area. In view of the fact that health information frequently moves between public and private sectors, and across jurisdictional boundaries, we agree that it is essential that a uniform set of principles apply to health information.

Given the key role that the proposed *Privacy (Health Information) Regulations* will have in providing guidance for privacy regulation in the health setting, we also strongly endorse the proposal for the OPC/APC to publish a document to bring together the proposed UPPs and amendments contained in the Regulations (Proposal 56-3) to ensure ease of access for users in this area. Similarly, we also support the proposal for the OPC/APC, with appropriate consultation, to develop guidelines on the handling of health information under the Privacy Act and the *Privacy (Health Information) Regulations* (Proposal 56-4). We believe that these strategies will help to ensure that the privacy principles, as applicable to health information, will be sufficiently transparent and identifiable to make this model workable.

In sum, we believe that it will be possible to progress the goal of harmonisation of health information privacy along the lines proposed in a manner which is compatible with an overarching national framework based on unified principles. Whilst this necessitates a process of qualification on the generally applicable UPPs through their amendment by the proposed *Privacy (Health Information) Regulations* which generates some additional complexity, we are satisfied that there are workable strategies proposed to ensure that the principles relevant for the health sector will be appropriately tailored to that sector and sufficiently transparent and identifiable. Use of guidelines, as distinct from legislation helps ensure flexibility for adaptation in the future to allow modification from time to time as appropriate. We are satisfied that this approach to privacy reform for the health sector addresses the suite of problems inherent in the current regime. In particular, we agree that this approach will help to minimise the compliance burden and associated costs. It will also help to clarify obligations for providers of health care services and minimise the complexity and confusion for consumers. We are confident that implementation of these changes will facilitate appropriate sharing of information which is especially important in the health care sector. We believe that this model will also help to break down the barriers for the conduct of research in the health sector.

We also note the proposed use of this model of using regulations to modify the UPPs in the context of regulating credit reporting and see merit in having a consistent model to create such modifications. We do note, however, that in that area, there is a proposed review of the proposed credit reporting regulations after 5 years of operation (Proposal 51-3) and we suggest that a similar review be undertaken of the *Privacy (Health Information) Regulations* to ensure fitness for purpose.

We support the proposal that the OPC/APC could delegate complaints handling to existing State and Territory Health Complaint agencies. This is consistent with the co-operative Federal Model and recognises the expertise already developed at the State and Territory level in complaints handling.

The Privacy Act and Health Information (Chapter 57, Proposals 57-2 to 57-10)

We strongly support the proposed amendments to the definition of health service to ensure that complimentary therapies are included. There has been a massive increase in the development, marketing and advertising of complimentary 'health' products and services. These service providers should be governed by regulations no less prescriptive than those applying to the traditional health service agencies and organisations.

Research (Chapter 58, Proposals 58-2 to 58-3)

We support the proposals for the development of a single set of rules covering the current Sections 95 and 95A of the *Privacy Act 1988* (Cth) (Proposal 58-1). The current NHMRC *Guidelines* are complex and still not fully understood by researchers or HRECs. ALRC Report 96 Recommendation 14.1 proposed that the NHMRC should review the *National Statement on Ethical Conduct in Human Research* to consider the mechanisms for achieving compliance with it, with particular regard to human research conducted wholly within the private sector. The latest version of the *National Statement,* coupled with the *Australian Code for the Responsible Conduct of Research* 2007 set out requirements for the development of a system of accountable research governance. The thrust of Recommendation 14.1 from Report 96 should be repeated as a supporting requirement for the development of research proposals in the current Discussion Paper. It is noted that Proposals 58-2 and 58-3 propose that the current *Privacy Act 1988* (Cth) provisions allow the use of personal information without consent with the approval of an HREC for health/medical research. Proposals 58-2 and 58-3 extend this HREC power. It is essential that the public have assurance that HRECs are acting in the public rather than the researcher's interest in the exercise of this important power.

We support Proposal 58-4 that the research exemption from the proposed UPPs for collection and use and disclosure continue to depend on the approval of an HREC being satisfied that the public interest in the research outweighs the private interest in privacy. This test has been used for many years and provides a proper balance between the public interest in research and the private interest in respect of privacy. We note that Proposal 58-6 requiring these research exceptions be approved by NHMRC will have administrative follow-up requirements for HRECs. In particular, we note the recommendations of ALRC Report 96 in relation to human research and the need to properly resource HRECs. The recording and reporting of decisions of HRECs to apply the research exception may require some further amendments to the current *National Statement on Ethical Conduct in Human Research* 2007. We also note and approve of Proposal 58-11 that the OPC/APC should prepare rules dealing with this important research exception and these rules should address the process by

which an HREC should review a proposal to establish a health information data base/register for research purposes. Similarly, we agree with Proposal 58-12 under which the OPC/APC will also include rules about how an HREC should review proposals dealing with data base/registers. The NHMRC will obviously have an important role to assist in the preparation of these rules. These rules will further operationalise Recommendations 18-1 to 18-3 of ALRC Report 96.