4 March 2005

JK: SJ
J. Kummrow
(03) 9607 9385
E-mail: jkummrow@liv.asn.au

Committee Secretary
Senate Legal and Constitutional Committee
Department of the Senate
Parliament House
Canberra ACT 2600

By Post and Email (legcon.sen@aph.gov.au)

Dear Committee Secretary

Inquiry into the Privacy Act 1988

The Law Institute of Victoria (***LIV***) welcomes the opportunity to provide a submission to the Senate Legal and Constitutional References Committee in its inquiry into the *Privacy Act 1988* (Cth).

We attach our submission, prepared with the assistance of a Working Party comprising members from the LIV's Administrative Law & Human Rights Section, for your review and consideration. Please note that an extension of time was sought and granted until 4 March 2005.

The LIV would welcome the opportunity to provide further submissions in relation to the issues raised our submission, should these be required.

If you would like to discuss any of the matters raised in the submission, please contact me or Jo Kummrow, Solicitor – Administrative Law & Human Rights Section on 03 9607 9385.

Yours sincerely

V.E. Strong

Victoria Strong
President
Law Institute of Victoria

Attach.

To: Committee Secretary, Senate Legal and Constitutional Committee, Department of the Senate, Parliament House

Inquiry into the *Privacy Act 1988* (Cth)

A submission from: Administrative Law and Human Rights Section of the Law Institute of Victoria

Date: 25 February 2005 (extension granted until 4 March 2005)

Queries regarding this submission should be directed to:

Contact: Jo Kummrow
Phone: 03 9607 9385
Email: jkummrow@liv.asn.au

Table of Contents

1. Background

In a letter dated 14 December 2004, the Law Institute of Victoria (***LIV***) was invited to make a submission to the Senate Legal and Constitutional References Committee's inquiry into the *Privacy Act 1988* (Cth) (***Privacy Act***).

The Privacy Act provides 11 principles governing the collection, use, storage, access to, maintenance and disclosure of an individual's personal information. These Information Privacy Principles (***IPPs***) apply to personal information held by Australian Government agencies. Since 1994, the IPPs have applied to Australian Capital Territory (***ACT***) agencies. The Privacy Act also contains ten National Privacy Principles (***NPPs***) that apply to parts of the private sector and all health service providers.

The LIV, through a Privacy Review Working Party of its Administrative Law and Human Rights Section, is pleased to make this submission to the References Committee and has given special consideration to the following matters set out in the terms of reference:

(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:*

(i) international comparisons,

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

(A) 'Smart Card' technology and the potential for this to be used to establish a national identification regime,

(B) biometric imaging data,

(C) genetic testing and the potential disclosure and discriminatory use of such information, and

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

The submission does not consider the Terms of Reference in relation to microchips that can be implanted in human beings or:

(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; and*

(c) the resourcing of the Office of the Federal Privacy Commissioner and whether current levels of funding and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate.

2. Summary of recommendations

The LIV recommends that the current privacy regime, as provided for under the Privacy Act, would be significantly improved with the enactment of the following legislative changes:

1. Minimum standards to be introduced in the Privacy Act to address:

(a) potential for barriers to international trade for business;

(b) lack of protection afforded to the consumer;

(c) effects on the take-up of electronic commerce resulting from lack of protection to consumers;

(d) lack of comprehensive coverage of business; and

(e) possibility that some states and territories will impose stricter privacy controls that may result in inconsistencies between jurisdictions"[1] (refer Section 3).

2. A requirement for public sector agencies and private sector organisations to prepare Privacy Impact Assessments upon the application of new technologies to business processes, goods and services where this will increase the collection, matching and sharing of personal information (refer Section 4).

3. Health information to be classified as sensitive information under the Privacy Act. A National Code to be introduced that sets out the minimum requirements for the handling of health and standard information; and information & communication technological requirements for the collection, use, storage, access to, maintenance and disclosure of an individual's personal information. Any such National Code should also address the requirements of the EU Directives. It is anticipated that the *National Health Privacy* Code should provide uniformity or greater harmonisation between public and private health sectors or between states and territories (refer Section 5).

4. The Privacy Act be amended to address the inadequacies identified by the European Union (***EU***) Data Protection Working Party and comply with the EU Directive (refer Section 6).

5. There are ways in which some new and emerging technologies are being applied to processes, services and products that represent a significantly high risk to privacy so much so that it is not sufficient to rely solely on the broad principles in the Privacy Act. The LIV recommends that more prescriptive, specific, rules are required (refer Section 7).

6. The LIV submits that the Privacy Act needs to be expanded to address the concerns about Smart Card technology and to also comply the EU Directive. One key concern is in relation to data mining (refer Section 8).

7. Biometric encryption systems are not, as yet, secure and are highly susceptible to infiltration by hackers. The LIV submits that current technology requires significant improvement and should not be introduced in the interests of privacy protection until the technology is less vulnerable (refer Section 9).

8. With respect to genetic testing, the following recommendations relate insurance companies and employers:

(a) Insurance providers and employers should be prohibited from using genetic information, or an individual's request for genetic services, to deny or limit any coverage or establish eligibility, continuation, and enrolment or contribution requirements.

(b) Insurance providers and employers should be prohibited from establishing differential rates or premium payments based on genetic information, or an individual's request for genetic services.

(c) Insurance providers and employers should be prohibited from requesting or requiring collection or disclosure of genetic information.

(d) Employment organisations should be prohibited from using genetic information to affect the hiring of an individual or to affect the terms, conditions, privileges, benefits or termination of employment unless the employment organisation can prove this information is job related and consistent with business necessity.

(e) Employment organisations should be restricted from accessing genetic information contained in medical records released by individuals as a condition of employment, in claims filed for reimbursement of health care costs and other sources.

(f) Violators of these provisions should be subject to strong enforcement mechanisms, including a private right of action (refer Section 10).

3. General comments

The LIV believes that the protection of an individual's privacy is fundamental to their human dignity and is central to most other human rights such as, the right of freedom of association, movement and speech, and in particular, rights protecting persons from covert surveillance and unwarranted intrusion.

As a consequence, the legal safeguards for privacy are scattered throughout the common law of Australia and federal and state legislation. The common law protects against trespass and breach of confidence, for example, and the Queensland District Court has recognised a general tort of privacy.[2]

Safeguards are also provided for in specific privacy statutes, which regulate the powers of law enforcement, security, health, education and welfare agencies and the activities of the administrators of other government programs. Privacy is also recognised in various statutes that regulate the private sector, including communications and anti-spam legislation.

The LIV submits that the Privacy Act, as a single piece of legislation, does not respond to new and emerging technologies. We suggest that it is often seen as a 'sword' and not a 'shield' in the way it protects the privacy of individuals in Australia. However, industry codes[3] (eg General Insurance Privacy Code and the currently unapproved Biometrics Institute Privacy Code[4]) allow various sectors to effectively and appropriately tailor the National Privacy Principles to the specific requirements for their industry sector.

The Privacy Act applies to the public sector and also to certain parts of the private sector. This submission focuses substantially on the effectiveness and appropriateness of the Privacy Act within the health sector.

The LIV notes that the Terms of Reference call for comments on the effectiveness of the Privacy Act in relation to certain new technologies. The Terms of Reference have restricted comments to new technologies including, Smart Card, biometric imaging, genetic testing and the use of microchips in human beings. However, the LIV recommends that the Inquiry

should be expanded to include the individual systems that support these new technologies. This is particularly relevant to the LIV's submission as a breach of privacy may not occur at the 'front end' or 'user end' (ie where Smart Cards are being used), but rather at the 'backend' (ie at the server where all the information is stored). We suggest that attacks on the backend of these systems are common and may result in a breach of privacy.

Further, the LIV submits that the introduction of the following minimum standards in the Privacy Act would provide a more streamlined approach to new technologies across all government, industry and business sectors and also address:

(a) the potential for barriers to international trade for business;

(b) the lack of protection afforded to the consumer;

(c) the effects on the take-up of electronic commerce resulting from lack of protection to consumers;

(d) the lack of comprehensive coverage of business; and

(e) the possibility that some states and territories will impose stricter privacy controls that may result in inconsistencies between jurisdictions".[5]

Subsequently, the LIV recommends that these legislative amendments should be implemented in each of the Approved Privacy Codes,[6] including a nationally consistent Health Code.

4. Privacy Impact Assessments

While the Privacy Act and its counterpart legislation in Victoria, New South Wales, Tasmania, Northern Territory and the ACT, require the public and private sectors to protect information privacy to minimum standards, it is overridden by any legislation that authorises an alternative standard of protection, whether higher or lower.[7] Further, there has been no inventory of the many statutory provisions that are inconsistent with specific privacy legislation. This means that it is difficult to determine how well governments are ensuring that privacy rights are not being inadvertently or unnecessarily eroded.

The current application of the Privacy Act is significantly broad. The LIV suggests that amid the enthusiasm to embrace the benefits of new technologies, the right to privacy can be dismissed as an impediment to progress or, alternatively, overlooked. Currently, there is no requirement for government to conduct an assessment of the impact on privacy (including possible inconsistency with privacy legislation) of or to justify any reduction in privacy under proposed new legislation. However, we note that the Office of the Federal Privacy Commissioner (***OFPC***) has voluminous publications relating to the impact of privacy, including media statements about determinations, case notes and review of private sector provisions.

The LIV suggests that a key issue is how to determine when compliance with the principles in the Privacy Act is sufficient, and when additional legislative protection is needed. We recommend that one solution is to require government agencies and organisations to prepare a Privacy Impact Assessment if they propose to apply new technologies in a way that entails collecting more information than before, sharing it more freely than before, using existing or new information for new purposes not envisaged before, or holding it longer than before. If the Privacy Impact Assessment reveals significant risks in the view of the Privacy

Commissioner, further regulation could be required, whether it be a code, regulations or new legislation.

We suggest that Privacy Impact Assessments will introduce a process under which due consideration should be given to the privacy rights of individuals in the context of other public interests, such as national security, law enforcement and administrative efficiency. Without a predictable, structured process to assess the privacy implications of proposals that could have a broad and significant impact on the community, each new idea is likely to attract controversy and criticism until the necessary analysis has been done. Some examples of controversial initiatives, where there has been a real or perceived failure to resolve the privacy issues so far, are set out below under each of the technologies listed in the Terms of Reference.

5. Privacy and the health sector

Health service providers document a timeline of a person's health care as well as social, demographic and other personal information in their clinical notes. Ongoing gathering of this information assists in diagnosis, provision of education, development of preventive health strategies, screening and, in some cases, conducting of research. Subsequently, a patient's health information is arguably a health provider's most important asset.

The LIV submits that there is a significant degree of confusion surrounding the operation of the Privacy Act and other privacy laws in the health sector.[8] Recent cases such as *KJ v Wentworth Area Health Service*[9] and *B v Private Health Insurer*[10] demonstrate the lack of understanding of fundamental privacy concepts and principles within the health sector. We suggest that this confusion does not arise solely from a misunderstanding by health professionals of the Privacy Act. Rather, it is exacerbated by the variation between federal, state and territory legislation. Such legislation is broader than the Privacy Act and includes the various freedom of information, state privacy and other health legislation.

Specifically, the LIV suggests that many health providers are uncertain about how to manage health information in a way that respects their patient's privacy and confidentiality. In the recent case of *Harvey v PD*[11] the NSW Court of Appeal upheld a decision against a medical practitioner to pay more than $700,000 to a patient in compensation. The case involved the Court scrutinising the medical practitioner's patient management system and their understanding of privacy and confidentiality obligations to a patient.

The LIV agrees that there are benefits and disadvantages to the introduction of new technologies. On the one hand, new technologies can benefit the health and welfare of individuals. However, the advent of new technologies may present new and complex legal issues. The focal point where health professionals, patients, researchers, statutes and information communication technologies meet is often highly scrutinised. The technology involved in health care is often scrutinised because the information is both sensitive and personal.[12] Furthermore, new technologies often facilitate the rapid movement of information between health centres and jurisdictions. The Privacy Act, along with many of the other laws, continues to struggle with the introduction of new technologies. However, the main difference between the Privacy Act and other statutes is the provision for organisations to enforce their own privacy codes.[13]

The approved privacy codes serve as an important mechanism for effective collection, use, storage, access to, maintenance and disclosure of an individual's personal information in each sector. Accordingly, codes need to be cognisant of the particular privacy issues

involved in each sector and the EU privacy directives[14] and known to the entire management and staff within an organisation. The old model used by the health professionals in the *Harvey v PD*[15] did not address the information management void and inevitably resulted in negative patient outcomes.

Once developed, a code needs to be regularly reviewed. This would facilitate diagnosis, education and research to be conducted and evaluated, preventive health strategies to be developed and screening to occur. If a code is not in place, the consequence of identification of mismanagement of health information after an adverse incident could be debilitating for the patient and a health professional.

Many publications assist health professionals to address the varying legislative requirements.[16] The OFPC has a number of effective publications that assist health professionals and individuals to access this information. The LIV submits that the OFPC has been receptive and approachable to the advocacy of privacy and development of information materials.

6. International comparisons

The Privacy Act was originally drafted with an eye to international standards of privacy protection. The preamble of the Privacy Act refers directly to the recognition given in the United Nations' *International Covenant on Civil and Political Rights*, the right to privacy, and to Australia's commitment to reflect in its legislation the 1980 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.

One of the Government's objectives in extending the coverage of the Privacy Act to the private sector in 2000 was to establish a scheme that was compatible with the *European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (***EU Directive***).[17] Compatibility would ensure that information about EU consumers could be transferred to Australian businesses without special conditions having to be put in place because the data would be protected to a similar standard under Australian laws.

According to the EU Data Protection Working Party of the European Commission (***Working Party***), which assesses the standard of protection provided by other countries against that provided within the EU, this objective was not achieved. In March 2001, the Working Party prepared a report that identified a number of inadequacies, compared to EU legislation,[18] most of which still exist.

The LIV submits that the most significant concerns include:

(a) Small business exemption: the Working Party said that, as it is difficult for a person overseas to determine whether or not an Australia business is exempt, it is necessary to assume it is.

(b) Employee data exemption: the Working Party recommended that operators exporting this data to Australia impose additional safeguards through special arrangements such as contractual clauses.

(c) The width of the exception permitting an organisation to use or disclose personal information for a purpose for which the person has not consented if it is 'authorised' by another law to do so.

(d) The exemption of data once it is publicly available.

(e) The ability of organisations to notify people that their data has been collected, and why, after it has already been collected.

(f) The ability to use and disclose information for direct marketing purposes, without the person's consent, if this was the primary purpose for which it was collected.

(g) The lack of special restrictions on the use and disclosure of sensitive information.

Accordingly, the LIV submits that Australia has not enacted legislation that protects privacy rights to the standard enjoyed in the EU, with the effect that the uncertainty that the legislation was intended to avoid continues to exist.

The LIV notes that, in response to a proposal put forward by Australia, an APEC Privacy Sub Group is developing a set of APEC privacy principles. The LIV suggests that it would undesirable if these principles were of a lower standard than currently reflected in the EU Directive, as it would exacerbate uncertainty among Australian businesses about which standards apply. For example, a business that collects personal information from customers in the EU, as well as Asia, might not be able to have the information processed in Asia.

7. Capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy

The LIV suggests that the Privacy Act, in its current form, is restricted in its capacity to respond to new and emerging technologies and the risks to privacy posed by such technologies.

The Privacy Act is based on general, technology-neutral principles that recognise the contextual nature of expectations in relation to handling of personal information. Namely, that what is sensitive in one set of circumstances may not be in another. While they can be improved, the Information Privacy Principles provide a useful framework within which organisations that hold personal information can understand their obligations and individuals can understand their rights.

The LIV suggests that there are ways in which some new and emerging technologies are being applied to processes, services and products that represent a significantly high risk to privacy so much so that it is not sufficient to rely solely on the broad principles in the Privacy Act. The LIV recommends that more prescriptive, specific, rules are required.

An early example is the *Data Matching Program (Assistance and Tax) Act 1980* (Cth), which contains detailed provisions to regulate the computer matching of personal information using Tax File Numbers. A more recent example is the *Spam Act 2003* (Cth) which addresses directly the emergence of commercial electronic messages. These statutes reinforce and build on the essential principles set out in the Privacy Act in relation to the collection, storage, use, disclosure, accessibility and destruction of personal information.

The technologies listed in the Terms of Reference are currently recognised as posing risks to privacy. The LIV suggests that the list be expanded to include other technologies, such as digital cameras in mobile phones, GPS technology, light x-rays of airline passengers and video surveillance, and drug testing and fingerprinting of school children. Even more items could be added as new technologies, and new ways of applying existing technologies, are developed.

We refer also to the recommendation set out above in section 4 on Privacy Impact Statements.

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

8.1 Background

A Smart Card can be described as a plastic card physically similar to a magnetic debit or credit card. However, beneath the surface of the card is an embedded integrated circuit or 'chip' that gives the card the ability to communicate, store and (in some cases) process data with a terminal.[19]

Smart Cards and the systems that support them are able to store vast amounts of information. This information may include banking details, store vouchers, Tax File Numbers, health records. Those in favour of Smart Cards believe that they improve customer service, operational efficiency and security for both the public and private sectors. However, the LIV suggests that Smart Cards also have the potential to become a technology of surveillance and control, which has previously been considered by government in a proposal to introduce a personal identification card in Australia (ie Australia Card).[20] The LIV submits that this generates new challenges for the privacy of individuals who use Smart Cards and organisations that manage the Smart Card system and utilise its information.

There has also been a proposal for the introduction of a Medicare Smart Card. At present an individual's MBS and PBS data and not linked. There is concern from both health professionals that there may be a threat to privacy if all three of these data sets are linked. Subsequently, the Privacy Act may need to be strengthened to ensure that this does not occur.

The LIV also notes that Smart Cards have been considered as driver licences, including, most controversially, in Queensland. Further, the use of Smart Cards for public transport has raised concerns about the collection of information about commuters and their travelling habits.[21][21] The use of e-tags for road tolls has also generated opposition where there is no option to use the roads anonymously.

The LIV submits that the current Privacy Act does not address the above overarching privacy issues and community concerns.

8.2 Technology and privacy issues

The LIV submits that the Privacy Act needs to be expanded to address the concerns set out in this section and follow the EU Directive. Article 25 of the EU Data Protection Directive[22] forbids any transfer of personal data from the EU to countries that do not guarantee or do not have in place adequate safeguards for such data. Currently, Australia is not one of these countries. Subsequently, Australian companies may be denied access to the EU market and health care companies stand to be most affected by this.

The LIV identifies the following concerns not currently detailed in the Terms of Reference or dealt with under the Privacy Act:

(a) what will the Smart Card be used for?;

(b) what information will be stored on the Smart Card;

(c) who has the right to use the Smart Card and have access to the information; and

(d) what is the role of the data in the Smart Card system.

Further, despite authentication of the user and host computer, the LIV suggests it is possible for an intruder to monitor a user-to-host connection and wait until all authentication procedures have been completed before attempting to intercept communications. The LIV recommends that encryption of all information passed between a user and a host is the most secure defence against such a threat.[23]

The LIV notes recent reports that the Australian Government's proposed document verification system to combat identity-related crimes (eg credit card and social security fraud) would be more effective than a system based on a single identity number. Federal and state government agencies and selected businesses, such as airlines and banks, would be able to verify the identity of clients by cross-checking birth certificates, drivers' licences and passports (with biometric identifiers) through an online central data exchange hub.[24]

The LIV further submits that Smart Card technology is susceptible to 'data mining'. This concern is particular relevant in the health sector where access to such a database would be immensely valuable to any organisation, particularly if MBS, PBS and the individual identification is linked.

9. Biometric imaging data

9.1 Background

Biometrics is the science and technology of measuring and statistically analysing biological data. In information technology, biometrics usually refers to technologies for measuring and analysing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.

The accuracy of technologies that collect and compare biometric data has been called into question. This has been controversial in view of the introduction of facial biometric features in passports in order to meet the requirements of the US Visa Waiver Program.

9.2 Technology and privacy issues

Biometrics has the ability to positively identify or authenticate an individual, thereby preventing a host of identity-related fraud issues, especially of concern now in an increasingly on-line world.

The biometric encryption system is vulnerable and highly susceptible to be infiltrated by hackers. Subsequently the system is not secure.[25] As a result, the LIV recommends that this aspect of the technology requires significant improvement to reduce its vulnerability before privacy can be discussed.

10. Genetic testing and the potential disclosure and discriminatory use of such information

10.1 Background

Genetic information is information about genes, gene products, or inherited characteristics that may derive from the individual or a family member. This includes family history. Genetic information pertains not only to an individual, but also family members and larger ethic groups.

There has been a recent inquiry into the use of human genetic information by the Australia Law Reform Commission and Australian Health Ethics Committee (***Issues Paper***)[26]. The Issues Paper recommended amending existing privacy laws to, amongst other things, prevent the misuse of the information. While the Issues Paper report has been commended nationally and internationally, the LIV notes that a response from the Federal Government response is pending.[27]

10.2 Technology and privacy issues

The LIV submits that genetic testing technology poses serious tensions between the interests of corporations and individuals. For example, women can now be tested to see if they carry a gene that makes them susceptible to breast cancer. However, many women many not wish to be tested because this information may affect their employment or deny them and their family access to certain health insurance policies. The LIV notes that diverse opinions exist as to who should benefit, hold, manage or be able to access this type of information.

In particular the Issues Paper raises a number of issues. These include emerging issues, ethical considerations, privacy, discrimination, medical and other human research, human genetic database, medical practitioners, health administration, employment, insurance, other issues, law enforcement and evidence.

The LIV's following recommendations, with respect to genetic testing, relate insurance companies and employers:

(a) Insurance providers and employers should be prohibited from using genetic information, or an individual's request for genetic services, to deny or limit any coverage or establish eligibility, continuation, and enrolment or contribution requirements.

(b) Insurance providers and employers should be prohibited from establishing differential rates or premium payments based on genetic information, or an individual's request for genetic services.

(c) Insurance providers and employers should be prohibited from requesting or requiring collection or disclosure of genetic information.

(d) Employment organisations should be prohibited from using genetic information to affect the hiring of an individual or to affect the terms, conditions, privileges, benefits or termination of employment unless the employment organisation can prove this information is job related and consistent with business necessity.

(e) Employment organisations should be restricted from accessing genetic information contained in medical records released by individuals as a condition of employment, in claims filed for reimbursement of health care costs and other sources.

(f) Violators of these provisions should be subject to strong enforcement mechanisms, including a private right of action.

Endnotes

[1] Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000, p 11.
[2] *Grosse v Purvis* [2003] QDC 151.
[3] See Approved Industry Codes at <http://www.privacy.gov.au/business/codes/>.
[4] See Biometrics Industry Privacy Code at <http://www.privacy.gov.au/business/codes/
[5] Revised Explanatory Memorandum
[6] Approved Privacy Codes are the codes approved by the Office of the Federal Privacy Commissioner in accordance with the Privacy Act.
[7] Privacy Act: Information Privacy Principles 10.1(c) and 11.1(d) and National Privacy Principle 2.1(g).
[8] Nihal Samararatna, 'Avoiding Uncertainty and Confusion with Health Information', *ADEA Magazine* Vol 8 No 1 March 2005. See also P Smith, 'Corporate threat to record privacy', *Australian Doctor* (28 January 2005).
[9] *KJ v Wentworth Area Health Service* [2004] *NSWADT* 84. See summary in [2004] *NSWPrivCmr* 7 (3 May 2004).
[10] *B v Private Health Insurer* [2002] *PrivCmrA* 2 (1 December 2002).
[11] *Harvey v PD* [2004] NSWSCA 97.
[12] Conditions are required to be met. See *Federal Privacy Commissioner Development Code Guidelines* (April 2001).
[13] EU Directive2002/58/EC of the European Parliament and of the Council of 12 July 2002. See also <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>.
[14] *Harvey v PD* [2004] NSWSCA 97.
[15] Nihal Samararatna, *Privacy Kit for Health Professionals (Diabetes Educators)*, World Health Federation (2005).
[16] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000.
[17] See <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp40en.pdf>.
[18] Michael Walters, 'Smart Cards and Privacy', *Privacy Law and Policy Reporter* (1994)
[19] Donna Bain, 'Smart Cards: A federal privacy perspective', *Privacy Law and Policy Reporter* (1996). It also evokes recollections of the failed attempt by the Australian Government to introduce the 'Australia Card' in the 1980s.
[20] A transport Smart Card is currently being trialed in New South Wales.
[21] John Woodward, *Fact Sheet on the European Union Privacy Directive*, Connecticut Department of Social Services (2000). See <www.dss.state.ct.us/digital/eupriv.html>.
[22] Tom Wright, 'Smart Cards: Executive summary', *Information and Privacy Commissioner*, Ontario (1993).
[23] James Riley, 'Privacy 'risk' in national ID plan', *Courier Mail* (21 January 2005).
[24] A Adler, *Vulnerablities in biometric encryption systems*, School of Information Technology, University of Ottawa (2005).
[25] Australian Law Reform Commission. *Issues Paper 26 Protection of Human Genetic Information List of Questions* (March 2003).
[26] Australian Law Reform Commission, *Annual Report 2003-04*, p 99.
[27] Above at 33, Chapter 4, Privacy of genetic Information.