Caroline Chisholm Centre for Health Ethics
7th Floor, 166 Gipps Street
East Melbourne, Vic, 3002
25/2/05

Submission in response to Parliament of Australia Senate Legal and Constitutional References Committee ***Inquiry into the Privacy Act 1988***

PREAMBLE TO SUBMISSION:

PRIVACY, MEDICAL CONFIDENTIALITY AND THE LAW

Doctor-Patient Confidentiality Essential

The need for doctor-patient confidentiality highlights an aspect of privacy required by a person's dignity, whose foundation is human nature, which encompasses a dual polarity, both individual and social. The undue disclosure of patient information is embarrassing and an offensive invasion of a person's privacy. The common good requires that the provision of health care be delivered with community trust in doctors to respect confidential patient information obtained during medical consultations. Little wonder there has always been a strong presumption in favour of the strictest confidentiality for patients' medical histories.

Community and Limits of Medical Confidentiality

With the growing sense of the community's social responsibilities in recent years the absolute character of this obligation has been questioned. The common good of the community that normally prohibits the disclosure of confidential patient information, may, in certain circumstances, require discreet disclosure to protect the same common good from serious harm. It would be unethical to protect a patient's confidence if this were to contribute to a serious injustice for an individual or the community.

Limits to medical confidentiality arise because a doctor has a specific and prior duty of care and protection for the health of the community **before** entering into any implicit contract of confidentiality with a patient. A doctor may not undertake an obligation that conflicts with a prior duty to prevent the unjust infliction of harm to the health of others. Doctors are recognised by the State as medical practitioners registered with the Medical Board to serve and promote the health of their patients as members of families and of the community.

The community expects doctors to have an eye to the public interest and not to be exclusively concerned with their own patients. To allay fears of irresponsible breaches of privacy or of doctors being rashly sued in the courts, community sanctioned criteria for the disclosure of confidential patient information to relevant individuals and/or authorities would need to be established and published. Discussions involving the community and doctors would help determine the sort of cases in which absolute professional confidentiality would not apply. For exsample, it is agreed that doctors are

ethically and legally required to inform public health officials of all cases of notifiable infectious diseases.

Medical Confidentiality and the Law

All other things being equal, patient confidentiality would not be morally binding if, as a last resort, disclosure to relevant persons was required to prevent unjust infliction of harm of a criminal nature in the community. This ethical duty of discreet disclosure arises regardless any eventual legal requirement. In practice, legislation may be needed to require all doctors to comply with this ethical obligation and to guarantee them legal immunity. In the absence of legislation some irresponsible persons might seek out doctors willing to maintain absolute confidentiality, regardless of any serious harmful consequences to the community. The law imposes mandatory reporting by doctors and other professionals who have reasonable grounds to believe a child is at risk of physical or sexual abuse.

Doctor-patient confidentiality must be maintained to the degree required for the community to retain its trust in doctors. A sign that a particular disclosure may be justified is to be found in the answer to this question: Would the community's trust in doctors be undermined if it were known doctors would disclose, as a last resort, confidential patient information to prevent serious harm to the well-being of an individual or the community?

Examples of Limits to Doctors' Confidentiality

There could be cases of patients whose serious medical condition, including a weak heart, deteriorating neurological co-ordination, poor eyesight, mental illness or drug addiction and which posed a clear threat of serious harm to an individual or the community in view of their occupation or continuing risky behaviour. Think of the case of a doctor who finds out that a pilot is no longer medically fit to fly an aircraft. The pilot might be reluctant to admit the seriousness of his/her condition, perhaps subconsciously influenced by the need to maintain the level of one's current income to meet payments for some months. The appropriate authorities should be informed once the diagnosis was confirmed to prevent risk of an air disaster. The same would apply to drivers of trains, buses or even motor cars, air traffic controllers and crane operators etc. A doctor through unjustifiable silence may not allow serious harm to be inflicted on the community.

There is a general duty to keep confidential a patient's HIV positive status because there is no risk of danger to others from a responsible HIV infected person who avoids risky behaviour. If, however, there were good reasons for believing that an uninfected non-consenting spouse or sexual partner was at risk of being unjustly infected, there would be a duty to disclose the relevant information to the appropriate person or authorities.

Medical Research

It does, however, seem that the public interest in protecting the right to privacy should be balanced against the community's interest in fostering medical research. It is one thing for researchers to have access to de-identified medical records and quite another to publish any identifying information obtained from such records, especially

if it could be embarrassing to the persons concerned. This latter case is to be absolutely avoided, unless required to prevent harm to the public or an injustice to an individual. Computer technology may provide the means to access patients' medical records without detriment to patients' privacy. For the common good it seems reasonable to facilitate medical researchers' access to **de-identified** information of medical records for epidemiological and medical research for improvements in the prevention and treatment of diseases without the need of obtaining consent from each patient. This could result in improved therapies, contribute to cost cutting for medical treatment for the community and the prevention of diseases in the population. The law should allow the NHMRC to modify its privacy guidelines to permit researchers access to patients' de-identified medical records without patients' prior consent for the common good.

Conclusion

The community expects doctors to report to the relevant persons in positions of authority cases where the risk of harm to the community or an individual is serious. There could be no reasonable objection to this. The trust of the community as a whole in the confidence of the medical profession would not suffer any loss if in extremely rare circumstances a doctor were to disclose a patient's confidential information to advise the authorities of a continuing risk of serious harm or abuse to an individual or the community. It is not a matter of doctors taking on the role of police officers but of responsible medical practitioners being true to their profession.

In the final analysis it is a question of assessing the balance of benefits and harms to the common good of the community caused by disclosure of, or failure to disclose, confidential patient information. The common good requires the presumption of absolute doctor-patient confidentiality unless disclosure was necessary in a particular case to prevent injustice or serious harm of a criminal nature to an individual or the community. Medical confidentiality exists for the community, not the community for medical confidentiality.

SUBMISSION

(a) The overall effectiveness and appropriateness of the Privacy Act 1988 as a means by which to protect the privacy of Australians.

- The notion of privacy is very much a subjective concept. What constitutes a threat to privacy is complicated. The common good is often cited as the reason for certain violations – in the interest of public or personal safety or national security.[1] D Solove[2] in attempting to conceptualise privacy states:

> 'A conception of privacy is different from the usage of the word "privacy". The usage of the word "privacy" constitutes the ways in which we employ the word in everyday life and the things we are referring to when we speak of "privacy". The word "privacy" is currently used to describe a myriad of different things: freedom of thought, control over personal information, freedom from surveillance, protection of one's

> reputation, protection from invasions into one's home, the ability to prevent disclosure of facts about oneself, and an almost endless series of other things.'

- Some ethical issues relating to privacy health care was discussed in a recent Chisholm Health Ethics Bulletin published by our centre, *The Caroline Chisholm Centre for Health Ethics*. It is attached as a separate **Appendix 1 for Inquiry into Privacy Act**: 'How private is our privacy in Health care', *Chisholm Health Ethics Bulletin* (Summer 2003) 9(2):1-4. Also available at www.chisholm.healthethics.com.au

(i) International comparisons

- Article 12 of The Universal Declaration of Human Rights states: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.[3]

- The European Commission states that 'we are all data subjects – whenever you book a flight, apply for a job, use a credit care, or browse on the Internet, -- you disclose some personal data'[4]. Following from this, the European Union specifies the following as a person's right as a data subject:-
  - You have the right to be informed of any data processing when you are the data subject.
  - You have the right to access data about you.
  - You must also have access to the logic on which automated decisions are based.

- The terminology adopted by Canada through their 'Personal Information Protection and Electronic Documents Act' may be useful. That is, *fair information principles*. In Canadian legislation, the public have the right to know and should ask why a business or organisation is collecting, using or disclosing their personal information. The *fair information principles* are seen as a balance between an individual's right to protection of personal information and the need for organisations to obtain and handle such information for legitimate business purposes.[5]

- The increasing use of the World Wide Web and Internet by individuals and organisations has implications for privacy, particularly if personal information is processed or exchanged via these networks. Human error may lead to inadvertent disclosure of sensitive information, which may have detrimental effects on individuals and organisations. Unlawful access to electronic sources of data is a worrying trend, particularly if it defrauds individuals and organisations, but especially if it threatens national and international security.[6]

(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

- A national ID scheme was not welcomed in the past, so another version of a national ID card is not really warranted. 'Smart Card' technology is currently being touted as new-age, inherently useful, and needed but the technology has been available for a few decades. Individuals already have the means to identify themselves with, eg. driving licences and passports which already provide photo identification, and medicare cards (which, similar to tax file numbers could arguably be considered a national ID scheme).[7] It would be reprehensible if the citizens of Australia have to carry ID as a legal requirement.

- A health care smart card for everyone is also not warranted. It may be useful to deter people who abuse the system and or travel extensively, and it may be beneficial to help identify people who are in accidents or are confused etc, but most of the population would not fall under these categories. Indeed they would be a very stable population who can articulate their health history, or parts that they wish to disclose, and not cause greater delays or expense to the health care system. Indeed it is the system itself that needs an overhaul, not the individuals who access it legitimately and in good faith.[8] However, if such a scheme is implemented in any guise (eg. with Medicare details) then people should have the option to be part of the scheme and consequently the option to opt out of such schemes. In addition, the individual who chooses to be part of the scheme controls what information is stored on the smartcard, and as far as possible, who can access it.

- Having sensitive health data stored on a 'card' and accessible via the use of a scanning/ reading device may help with data-flow but will not ensure the privacy of the individual is maintained. The same conditions that currently dog the handling of health information will persist, but with added problems, such as may occur if people forget to bring their smartcard, or lose it, or have it stolen or loan it to someone![9]

- There is also the concern that there may be unauthorised access to the information on the smartcard and the risk that the information will be used and transmitted without the person, whose information it contains, consent.[10] In the event that such use for 'smartcard' technology is approved, can the legislation protect the individual in maintaining control of their own smartcard. For example, it is not unusual for pharmacies to take an individual's medicare card whilst processing a script. The individual, in this instance, no longer has control over what occurs with his card whilst the pharmacy has custody over it, even though it may be for a limited time and the card is eventually returned. It would be of greater concern if this occurs with 'smartcard' technology which contains both personal and sensitive data.

- In addition to the above is the possibility for smart cards being used for incremental information (such as was proposed for the Queensland Drivers licence recently), such as licensing, insurance, health, financial etc.[11]

- Smartcards may actually impede data flow if the individual chooses not to use them in a system reliant on them. Not producing a smartcard may lead to exclusion in various organisations, or limit access, eg. to medical care.

Unauthorised use or use beyond the original intention may jeopardise an individual's trust with certain organisations, the health care system in particular.

- The legislation needs to be specific about any device that may fit under the category of smartcard. This includes not allowing loopholes by exploiting the terminology. That is, when is a card not a smartcard? When it is a key-ring, or a microchip, or a band around a wrist etc. If biometric data is included then the smartcard becomes a potential identification, authentication and forensic tool as well as a databank in its own right.[12]

- The legislation should take care not to accept smartcard technologies which impinge or breach the privacy principles, especially in the sphere of data-matching etc. Whilst it is useful to discuss the various technologies of smartcard, biometric imaging and microchipping separately, they are all inherently the same in principle with the same potential for exploitation, discrimination, and unwarranted erosion of people's personal privacy.

- The use of radio-frequency identification (RFID) technology also needs consideration. Its reported use in retail has raised concerns about privacy.[13] Whilst the products we buy are not private once we use Eftpos or credit card facilities, the use of (RFID) has wider implications.

- Other concerns is the potential for some smartcards to be used as tracking devices (perhaps via radio frequency capabilities or global positioning satellites) without the consent or awareness of the individual.[14]

B. Biometric imaging data

- The legislation does not specify for what purposes biometric imaging data is needed. Discussion has centred on its use in passports.[15] Biometric imaging is also used in some employment situations and educational institutions.[16] As with smardcard technology, its use is not compellingly warranted.

- However, in the event that biometric imaging becomes a condition of access to certain services etc, then the issue of compliance with such schemes needs discussion before biometric imaging becomes legislative fact. Biometric technologies have been described by privacy experts as 'an extremely dangerous form of social control, extremely inappropriate and seriously damaging to our freedoms'[17]. Consent issues need to be considered. There may be a degree of coercion, and thus civil liberty losses if people feel threatened into joining 'biometric imaging' schemes, because of fear of loss of certain conditions, such as employment, medical care, the freedom to travel etc. Opt-in or opt-out conditions need consideration, as well as type of biometric data to be captured or stored.

- As with smart card technology and microchip implants, the problem arises of what information will be captured, for what purpose and for whose access.[18] Will such information, once scanned, be stored on a database every time a biometric image is processed. Will the potential for anonymous transactions be eliminated. There should be public debate about all such technology if it is proposed to be

used for identification/ verification/ or matching purposes, especially for the likely false negative and false positive scenarios that are a flaw in all identification/ verification/ and matching schemes.[19]

- Another concern is the potential to capture both genetic information and biometric information within a smartcard-like device that can be implanted. This is not science-fiction but technologically possible. Will the legislation be able to deal with this threat to the privacy and liberty of the general public.[20] The public are already under frequent and unnecessary surveillance without their knowledge or consent.[21] Information about us is collected through the use of other smartcard technology that changes in banking and retail have encouraged us to use. For example, Direct Marketers target us after information about our shopping habits, as revealed by products we purchase with Eftpos or credit card, is retained in data-bases and sold to organisations wanting our custom.

- There is no compelling evidence that capturing biometric data will improve privacy or security.[22] People are already required to give various levels of evidence that they are who they purport to be before accessing some services. Identity theft and fraud is problematic in current usage of 'smartcard' technology. Using biometric data will not prevent this, but perhaps make it more difficult for the person whose identity is stolen.

- It is a concern that once captured, biometric data may be used for secondary purposes, beyond verification and identification. The legislation should prohibit extending the use of biometric imaging data for national identification purposes.

- Some ethical issues relating to biometric technology in health was discussed in a recent Chisholm Health Ethics Bulletin published by our centre, *The Caroline Chisholm Centre for Health Ethics*. It is attached as a separate **Appendix 2 for Inquiry into Privacy Act**: Ref: 'Privacy, Biometrics, Technology and Health', *Chisholm Health Ethics Bulletin* (Autumn 2004) 9(3):4-6. Also available at www.chisholm.healthethics.com.au

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

- Genetic information, whilst used predominantly for medical purposes, also has implications beyond being medical information. Technology capable of determining genetic disorders and predisposition to certain conditions and behaviours continues to be developed for research.[23] This technology may possibly be developed as lucrative commercial enterprises. The legislative regime would need to cover current developments and anticipate future capabilities.

- Because a DNA sample contains information which can have implications not only for the individual but for their family, the legislation needs to be specific about consent to obtain sample, consent to test sample, consent to store sample and any information derived from the sample.[24] It also needs to anticipate unforeseen or yet to be developed technology which may be used to glean more information from stored samples. Large-scale genetic testing of various

populations should be prohibited, especially on vulnerable groups such as children, and ethnic minority groups.[25]

- The use, ownership and storage of samples, such as those obtained in new-born screening programs appears contentious.[26] This needs clarification at a national level.[27] Given the reports of human tissue specimens stored (and sometimes) removed without an individual or parental/ guardian consent it would be useful to address this in the legislation since it has implications for the privacy of the families involved.[28] This is an area that needs urgent legal clarification.

- An individual should not be obligated or coerced to disclose genetic information about themselves even if it may have implications for other members of their family. However, if a genetic test reveals that a woman has a serious inherited genetic defect that would affect one in four or even one in two of her children, this information should be revealed to her female sibling who would have the same genetic defect as this information would be very pertinent for reproductive options. Normally this information would be willingly passed on in a family. If the woman refuses, the health professionals should try to persuae her to reveal it. If she still refuses, the law should permit this information to be passed on: it is not merely an individjual's genetic information, but family information that should be shared for very good reasons. Family members in general should not be able to access genetic information of another family unless that individual consents to this disclosure. Exceptions to this must be specific, eg: minors and those deemed incapable of giving informed consent, crime detection and ensuring that innocent people are not convicted of crimes they did not commit. In these instances the genetic information should not be retained beyond its original purpose. In particular, DNA evidence of convicted criminals only may possibly be retained. All those cleared of convictions should have their DNA samples destroyed and any information pertaining to the sample removed from the data-base.

- If an individual consents for their identifiable genetic information to be used for research purposes, then this has implications to their wider family who should also consent or have the right to decline to consent. There should be an all or nothing principle used in this situation. That is, everyone who might be effected by the results of the research needs to consent. If one person declines, then that information cannot be accessed or used for secondary purposes or third-party disclosure. Because of the information that can be derived from genetic material, it would not be useful for an individual to give a universal waiver to the use of their genetic information. The legislation needs to be specific about consent requirements. However, it would be different if the genetic information was irreversibly de-identified.

- The legislation needs to be specific about non-consensual testing other than the conditions allowable for criminal investigations. That includes making invalid any claims made by persons who 'steal' genetic material left by an individual, eg. shed hair, and tests it without that individual's knowledge. There should be legal clarification about what rights individuals have in regard to paternity claims made against them, even with genetic proof, when it is established that genetic testing has occurred without their consent. Court approval should be required for paternity tests to have legal validity where one parent refuses consent. Society

highly prizes genetic privacy, but society and the law should not be involved in collusion with perpetuating cases of paternity fraud. The law shojuld also in such cases attend the well-being of children.

- The requirement of genetic testing for insurance purposes should be banned. Any testing for predisposition to medical conditions, especially 'lifestyle and behavioural' ones such as alcoholism, should be prohibited. Genetic testing for employment, education, sporting and recreational discrimination should be prohibited.[29] Genetic testing to aid law enforcement needs public debate to determine its legal parameters.[30]

- Potential sources of genetic information, such as sites which store newborn screening (Guthrie) cards, should not remain in the private sector. If the legislation will not allow destruction of the samples after they have been used for their original purpose then they need to be secured and 'stored' in a manner similar to information stored with Medicare and Pharmaceutical Benefits. That is, each sample has an individual PIN.

- This paragraph pertains to newborn screening but could be applicable in other situations where a biological specimen is obtained. Prior to obtaining a specimen consent is needed. This should be fully informed, that is: why the test is needed; type of tissue needed; where tested; type of results; how results reported; disclosure to other parties (eg. medical specialists, or for disease notification under the Medical Treatment Act). In addition, the individual should receive the results, and have authority about what happens to the information and the specimen after the initial testing. The individual may choose to relinquish ownership of the specimen and thus any rights to what subsequently is done with it. However, this does pose a dilemma because genetic material has implications beyond the individual. This may mean having the specimen returned to them, destroyed, or stored in an identified or de-identified manner for secondary purposes to which they agree to, eg. general or specific medical research.[31] For example, an individual may be willing for their genetic sample or information to be used to aid in medical research but not agree if their genetic sample or information is used for purposes they would morally oppose, such as encouraging eugenic-type discrimination.

- Given that genetic information is being obtained from such sources as newborn screening (Guthrie) cards without fully informed consent, then legislation should be enacted to halt such secondary use until the public is made aware of the intent to test their genetic sample and use their genetic information. There should never be an assumed 'free for all' access to those wishing to do any type of research using stored genetic material.

- There is a concern that genetic information is being exploited for commercial profit which does not benefit the individual who supplied the sample. For example, commercialising a unique type of cell-line derived from someone's tissue sample. This has some historical precedents[32], but needs to be addressed in the legislation.

- Employers and insurance agencies should be prohibited from accessing any genetic database for any purpose. Employment or insurance should not be made conditional on any individual needing to disclose or relinquish a genetic sample for testing purposes.[33]

- The development of various data-banks which contain genetic information needs regulation or monitoring by an authorised organisation such as The Privacy Commission. Because all possible future research questions are unknown, it is difficult to condone carte blanche use of genetic material infinitum. Implementing an 'authorization model policy'[34] has been proposed to allow participants to exercise control over future uses of their genetic material.

- A potential problem with having various data-bases, especially electronic ones, is their use to match data. Therefore any current or proposed policy that allows 'data-matching' needs to be addressed in the legislation.[35] The public need to be fully informed of any plans that will allow their data to be linked with other data, since this builds up a profile of an individual which may not always be used in their best interests. Western Australia allows some data to be linked.[36] However, it is unclear whether the data is being used beyond its original intent and for secondary purposes which the public have not consented to or are unaware about.

D. Microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration)

- Implanting microchips into humans for the purposes of identification, verification, matching, surveillance, restraining or tracking should be prohibited. Suggesting that implanting microchips would be useful for monitoring the movements of vulnerable populations, such as young children or individuals with dementia is not persuasive as it impinges on the civil and moral right of an individual not to be under constant surveillance.[37] There are less invasive means of monitoring an individual.[38]

- At present, the use of implanted microchips in humans seems limited to securing access to restricted sites by authorised personnel.[39] Using microchip implants for identification will not stop identity theft. Implanted devices may be used beyond their original intent eg, that is tracking persons movements via RFID technology.[40] There may be a need to monitor certain people, such as prisoners in alternate forms of custody outside the penal system, with attachable devices. If there is a plan to introduce implanted surveillance devices, then this needs public debate and legal clarification.

- If implanted chips carry information that is considered sensitive and/ or personal, will the legislation be powerful enough to deter unauthorised access to this information by scanning devices and those accessing and using these devices. Will the 'chipped' individual have control over what information is stored in the device, who may access it, down-load it, add to it, delete it etc. It would not be unreasonable to assume that data can be modified on the chip.

- The potential for adverse medical effects posed by such devices needs to be considered.[41]

- Implanted microchips take away an individual's right to remain anonymous in all respects and is a violation of their privacy. Will the legislation be rigorous enough to deter the potential for unlawful remote tracking of the device (also applicable to 'smartcard' technology).

- The same concerns raised by smartcard technology and biometric imaging also apply with implanted devices, such as being wrongfully excluded or discriminated against, being denied access to services, such as medical care, and being miss-identified which may lead to unlawful detention or wrongful conviction for criminal activities etc. It is accepted, that such devices would aid identification in certain populations but only in limited circumstances, eg., lost persons suffering dementia or following an accident.

- Will the legislation, along with the Criminal Act, protect the individual, if hackers find a way to unlawfully access the information contained in the microchip.

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

- There are some exceptional circumstances where the legislation needs to be flexible to allow some unrestricted data-flow. For example, in medical emergencies where urgent information is needed to aid diagnosis and treatment and obtaining consent is impractical. Another situation arose recently following the Tsunami event where privacy legislation may have been a factor in delaying identification of deceased persons. It would be helpful if the revised legislation considers 'fair information' principles.

- Is it possible to include other aspects of privacy law, such as that to do with telecommunication, surveillance, health information, spam, direct marketing etc, to come under a single jurisdiction. Surely the ad hoc nature of the various laws which have privacy provisions creates the potential for 'loopholes' in legislation to be exploited.

- The federal *Crimes Act* needs updating.

- There is a lot of legislation covering bits and pieces of privacy in Australia, not-withstanding the various privacy legislation enacted by the different states and territories.

- Differentiate or clarify which breaches of the Privacy Act may constitute a criminal act as opposed to breaches which can be pursued through the civil law courts.

- It would be beneficial if there was one overall national Privacy Act, which covers all aspects of privacy throughout Australia. That is, the state legislation could be over-ridden or be repealed.

- It would be useful to have one overall federal *Whistleblower* legislation, given that the states have different provisions for this, with markedly different levels of protection.

- It would be useful to have one overall federal *Freedom of Information* legislation which covers all freedom of information law in Australia. That is, the state legislation could be over-ridden or be repealed.

- The law needs to adresss the use of photographing persons without their consent. The matter arises in the first instance at the beach where sun-bakers may be topless. The beach is a public place and a passer-by may look about. Sun-bakers implicitly permit this, but this does not mean somebody should stop and gaze intently at a topless woman on the beach. This would be harassment and offensive behaviour, and then police would ask the passer-by to move on. The case scenario here is limited to a particular time and place. Taking photos removes the image of , say a topless woman, away to hundreds of other potential locations and times without her consent. Think of digital cameras and the Internet!. This is an invasion of privacy and offensive. Taking photos of people walking down the street would not generally be offensive and consent may be presumed unless the photographers behaved offensively. The same applies to TV images of the crowds at cricket, football or the Australian Tennis Open. The key thing to ban phtographing persons without their consent or presumed consent in public places where no harassment could be suspected. Why should people coming out of court case have to cover their heads with a bag? Taking photos here is also offensive to the person involved and should be banned as intrusive of privacy. "Consent" and "harassment" are key concepts for regulating this area..
- The privacy of citizens against whom criminal allegations have been made, when no charges has been laid should be respected until charges have been laid. Some newspaper reports can ruin an innocent person's reputation by publishing such damaging reports. Once charges are laid, public interest would justify publicity in newspapers. Privacy legislation should innocent persons in such cases.
- Phone tapping: this should be illegal unless done with the approval of a court or strictly in accord with law, say anti-terrorism laws. … this also applies to the police.

(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

- All organisations, as defined by the act need to comply, including small businesses, regardless of how many millions of dollars they turnover.

- Employee information should not be exempt from privacy legislation.

- The two issues above have been highlighted as flaws in the Australian legislation in commissioned reviews.[42]

- The dialogue about Privacy Codes is confusing. There should be one national over-arching basic Privacy Code that applies to all sectors. If organisations wish to develop their own codes then these must be in addition to the principles in the basic National Privacy Code. This would then allow the legislation to guide legal case law, if an organisation breaches the basic privacy code.

(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.

- It would be useful to extend the powers of the Federal Privacy Commissioner into the states, which would be possible if there was one overall national Privacy Act covering all aspects of privacy in Australia.

- The position of Federal Privacy Commissioner should be a dedicated commission, without the incumbent having responsibility for other portfolios, nor have employment outside of the position. If there was one overall national Privacy Act covering all aspects of privacy in Australia, then it would warrant deputising State and Territory Privacy Commissioners who are answerable to the Federal Commissioner.

PLEASE SEE TWO ATTACHED ARTICLES PUBLISHED BY OUR CENTRE IN TWO APPENDICES RELEVANT TO OUR SUBMISSION

APPENDIX I: "How private is our privacy in health care?"

APPENDIX II: "Privacy, Biometrics, Technology and Health"

Endnotes

[1] L Nelson, 'Protecting the common good: Technology, objectivity, and privacy', *Public Administration Review* (2002) 62:69-73.
[2] D Solove, 'Conceptualizing Privacy, *California Law Review*, (2002) 90(4):page 5 of 60.
[3] United Nations Universal Declaration of Human Rights, http://www.un.org/Overview/rights.html accessed 21/2/05.
[4] European Commission, *Data Protection in the European Union*, http://europa.edu.int/comm/represent_en.htm accessed 17/2/05.
[5] www.privcom.gc.ca/legislation/02_06_07_e_asp, accessed 7/2/05; A Gounaris, B Theodoulidis, 'Data Base Management Systems (DBMSs): Meeting the requirements of the EU data protection legislation',' *International Journal of Information Management*, (2003) 23:185-199; .
[6] M Whitman, 'In defence of the realm: understanding the threats to information security', *International Journal of Information Management*', (2004) 24(1):43-57; M O Reilly, 'Your secrets aren't sacred', *Canadian Medical Association Journal*, (1999) 160(13):1859; R Sikorski, R Peters, 'A Privacy Primer for the Web: Spam, Bread crumbs, and Cookies', *JAMA*, (1998) 279(15):1219-1220.
[7] R Ackland, 'There are bigger threats than ID cards', *Sydney Morning Herald*, www.smh.com.au accessed 7/2/05; Asia Pacific Smart Card Forum, *Smart Card Technology*, www.smartcardforum.asn.au/smartcard.htm accessed 7/2/05;
[8] Australian Government Department of Health and Ageing, Media release, *Medicare smartcard launched*, 28/7/04; AustLII, *Medical Record Cards*, www.austlii.edu.au/au/other/CyberLRes/1995/smart/42.html accessed 7/2/05; IDA, Unknown author 'Italy launches electronic health card', *eGovernment News* 12/1/05, Italy, http://europa.eu.int/idabc/jsps/documents/dsp accessed 31/1/05.
[9] J Riley, 'Privacy 'risk' in national ID plan', *Australian IT*, 21/1/05, http://australianit.news.com.au accessed 31/1/05

[10] C Nader, 'E-card may hold key to good health', *The Age*, 29/1/05.
[11] Queensland Government, *Licensing*, www.transport.qld.gov.au/new_driver_licence accessed 17/2/05.
[12] J Riley, 'Privacy 'risk' in national ID plan', *Australian IT*, 21/1/05, http://australianit.news.com.au accessed 31/1/05
[13] A Gilbert, *Privacy activists call for rules on RFID*, http://www/zdnet.com.au/news/business/0,39023166,20277505,00.htm accessed 14/2/05.
[14] A Gilbert, *Privacy activists call for rules on RFID*, http://www/zdnet.com.au/news/business/0,39023166,20277505,00.htm accessed 14/2/05.
[15] 'Australia could be first to use biometric passports', *The Age*, 5/6/03.
[16] 'Biometric identification raises privacy concerns', *Sydney Morning Herald*, 9/9/03, www.smh.com.au accessed 12/9/03.
[17] R Clarke cited by K Arlington, 'Biometrics dangerous: expert', *news.com.au* accessed 9/9/03, http://www.news.com.au accessed 7/11/03.
[18] F Pierce, 'Biometric identification', *Health Management Technology*, (2003) 24(5):38.
[19] R Hopkins, 'An introduction to biometrics and large scale civilian identification', *International Review of Law, Computers & Technology*, (1999) 13(3):337-363.
[20] W Green, 'Biometrics and the law: what law?', http://www.lawyersweekly.com.au 21/5/04, accessed 7/2/05.
[21] R Franklin, 'Forget privacy, just watch Big Brother', *The Age*, 2/2/03.
[22] A Salkever, 'Why biometrics is no magic bullet', *BusinessWeek online*, 22/7/03, http://www.buninessweek.com accessed 21/2/05.
[23] Gene Technology Information Service, *General information and Fact sheet 20 Genetic testing and privacy*, www.biotechnology.gov.au October 2004, accessed 7/2/05.
[24] J Robotham, 'Parents not told about gene risks', *The Age*, 3/7/04.
[25] GeneWatch UK, 'Bar-coding babies: Good for health?' GeneWatch UK Briefing Number 27, August 2004, http://www.genewatch.org accessed 20/12/04.
[26] N Curtis, *Newborn screening cards safe, says genetic service*, Media release, Murdoch Children's Research Institute, 5/7/04, http://www.mcri.edu.au/pages/news/release47.asp accessed 18/2/05; T Noble, 'Law may resolve blood sample issue', *The Age*, 6/7/05; 'How your DNA is falling into private hands', *The Age*, 5/7/04.
[27] Human Genetics Society of Australasia, *Policy Statement on the Retention, Storage and Use of Sample Cards from Newborn Screening Programs*, HGSA Policies, No date, http://www.hgsa.com.au/policy accessed 18/2/05.
[28] S Taub et al., 'Safeguards in the use of DNA databanks in genomic research', *Genetics in Medicine*, (2004) 6(6):526-529.
[29] M Otlowski, 'Emerging legal issues in relation to the use of genetic testing: An examination of the phenomenon of genetic discrimination', *Plaintiff* (2003) 55:29-34.
[30] Author unknown *Police DNA database attacked by Gene Watch*, 14/1/05, www.outlaw.com accessed 17/2/05.
[31] OECD, *Main points from the OECD Workshop on 'Human Genetic Research Databases – Issues of Privacy and Security* 26-27/2/04, Tokyo, Japan, http://www.oecd.org accessed 11/2/05.
[32] P Roughan, *The diversity resource? Genetic research in Pacific Island futures*, The Foundation for Development Cooperation, no date, http://www.fdc.org.au/files/roughan-2.pdf accessed 17/2/05.
[33] M Stulic, 'Genetic Non-Discrimination, Privacy and Property Rights', *Murdoch University Electronic Journal of Law*, (2000) 7(2) http://www.murdoch.edu.au accessed 17/2/05; E Wright, 'Genomic Medicine: Ethical, legal, and social implications of Genomic Medicine', *The New England Journal of Medicine*, (2003) 349(6):562-569.
[34] T Caulfield et al., 'DNA databanks and consent: a suggested policy option involving an authorization model', *BMC Medical Ethics*, (2003) 4(1).
[35] R Magnusson, 'Data linkage, health research and privacy: Regulating data flows in Australia's health information systems', *Sydney Law Review*, (2002) 24(5)5-55.
[36] C Garfield et al., *Inside the Western Australian data linkage system*, Symposium on Health Data Linkage, 20-21 March 2002, Sydney, http://www.publichealth.gov.au/symposium.htm accessed 17/2/05, p. 78-81.
[37] M Wertheim, 'Someone to watch over me', *The Age*, 7/7/02, http://www.theage.com.au/articles/2002/07/06/1025667073515.html accessed 21/2/05.
[38] E Schonfeld, 'Meet the cyborgs next door', *IT in Government*, 3/7/02, http://www.zdnet.com.au accessed 21/2/05.

[39] W Weissert, 'Microchips implanted in Mexican officials', *MSNBC*, 14/7/04, http://www.msnbc.msn.com accessed 31/1/05.
[40] W Weissert, 'Microchips implanted in Mexican officials', *MSNBC*, 14/7/04, http://www.msnbc.msn.com accessed 31/1/05.
[41] D Appell, 'Getting under your skin', *Scientific American*, (2003) 288(1):18.
[42] Article 29 – Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, Adopted 26/1/01, The European Commission, www.europa.edu.int.comm.dg15/en/media/dataprot/index/htm accessed 17/2/05.