Submission to the Australian Law Reform Commission Inquiry into Privacy Legislation

Introduction.

In any society in which there are bureaucracies, public of private, there is reason for people to be concerned about what information, and what misinformation, is being held, and what decisions are being made that are based on that information. There is reason to be concerned that information that was provided for one purpose, and so is expressed to suit that purpose, may be used for another, where it is misleading. There is reason to be concerned about data matching, when false conclusions may be drawn, wherever there is inadequate consultation of the subject of the data.

In any society in which there is prejudice, there is reason for people to be careful of what information about themselves is publicly disseminated. In Australia, where the Work Choices legislation has meant that many employees are open to dismissal without good cause, there is fresh reason to be concerned.

Recent and proposed changes in legislation are worrying. The multiple collections that will be accessible through the proposed Access Card, and that are proposed in the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006, will substantially increase the risk of misuse. Changes to the Telecommunications (Interception) Act, the Surveillance Devices Act and other anti-terrorism laws, have turned laws which were originally designed to protect privacy into ones which authorise substantial invasions. The Families, Community Services & Indigenous Affairs & Veteran's Affairs Legislation Amendment Act 2006 permits both invasion of people's homes and data matching, with people at risk of having their government support removed, before they have an opportunity to challenge the conclusions that are drawn about their entitlements.

Restrictions on what can be done with personal information should be a matter of law, not merely of regulation, departmental instructions or convention.

More and more private organisations are collecting data that they do not really need. A culture is being created in which organisations as a matter of course want information that is not relevant to their purposes. Clubs want to photocopy your divers' licence. Gymnasium clubs take your photographs. Banks want to know your mother's maiden name. Obtaining an e-tag from the NSW RTA requires the provision of substantial information. (And there is not much choice—on toll only roads, the alternative is a substantial increase in travelling costs.)

To deal with these changes, it is essential that the basic principles privacy are supported by law. In particular, information that is collected for one purpose by one agency or organisation should not be available for another purpose, or transferred to another agency or organisation—or, indeed, another part of the same agency--without a fresh consent being given and fresh opportunities for input and comparison.

Principal comments and recommendations

1. Privacy is not a right that can be held by a group.
2. The Privacy Act should be amended to create a tort of privacy.
3 .Of great importance is the ability of people to control their personal information. It should be possible to obtain an injunction from a tribunal, that changes must be made to a record or a web site, or that other breaches of privacy must cease, or that compensation is due.
4. There needs to be a raft of remedies, including having information corrected, having misinformation and old information removed, having information for which the holder has no entitlement removed, having such changes passed on to those who have acquired material from the primary users, instead of or as well as financial compensation.
5. There should be a tort of intrusion, too.
6. The new system needs to be based on principles that can continue to be applied as technology changes.
7. We accept that the legislation will need to allow exceptions to be made in order to provide protection of people in danger, and information to their relatives. Travellers should be asked in advance for permission for this to be done.
8. There is no automatic right of parents to know about the medical or educational problems of their children. This is an area where the law needs to be flexible, for the age of the child and the nature of the problem determine what is appropriate.
9. The norm for medical research should be that informed consent to publicity and to retention of personal details is required, just as it is for the research itself.
10. Similar requirements should be placed on social science researchers. The reasons for privacy are even more cogent, because of the effects of their research upon minority and disadvantaged groups.
11. Small businesses may need special handling to avoid the imposition of unreasonable burdens. But that should not require a blanket exemption.
12. Subject to the constitutional right to freedom of political communication, political parties should be forced to comply.
13. Rather than there being a blanket exception, a code specific to the media should be developed, by which they should be bound.
14. Every parliamentary bill that affects human rights, including privacy, should require a human rights impact statement. This should occur, no matter how indirect the effect is.
15. The only information that should be held by credit agencies is whether or not a person has defaulted on repayments. A lender will examine the borrower's current income and commitments. Nothing else is relevant. The procedures of credit agencies and lenders should be strictly regulated, if necessary by a separate piece of legislation.
16. There need to be multiple restrictions on the use of data which has been collected for one purpose, for another purpose. Such transfer should only be done with the knowledge and consent of the subject of the data.
17. The International Covenant on Civil and Political Rights gives the Commonwealth power to legislate to protect privacy. That power should be used, in the interests of consistency, and more importantly, to set high minimum standards.

The states should be able to add their own laws, to suit their own circumstances, that apply above the minimum Commonwealth privacy framework[1].

1. Privacy and groups.

Privacy, in our submission, is not a right that can be held by a group.

1.1 There are rights that are held by all members of a group, in virtue of some characteristic that they hold in common, and a universal right to which the characteristic is relevant. But hat entitlement is not an entitlement of the group (the set of individuals) but of each of them separately. While the right of privacy may be common to a group it is inherently an individual right and must be enforced individually. The effect of a breach of privacy on a group should be used as an aggravating factor in the calculation of remedies.

1.2 Similarly, the entitlement that the men or women of an Aboriginal nation have, that each member will maintain secrecy concerning their men's or women's business, is an entitlement held by each individual over each other individual.

1.3 The situation may be contrasted with traditional Aboriginal land rights. These are rights that are held by nations, and they are not analysable into individual property rights.

1.4 The arguments for the right to privacy appeal to characteristics of individuals, not to characteristics of groups. Privacy is a matter of respect for an individual's autonomy, a requirement of developing and maintaining relationships, a prerequisite of personal development, a requirement for psychological health, a prerequisite for spontaneous interaction and so forth. These are characteristics of individuals, which groups do not share. None of these imply a moral entitlement to group privacy.

1.5 Similarly, the basis for a legal entitlement in international law lies in the *International Covenant on Civil and Political Rights*, the *Covenant on the Rights of the Child*, the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Persona; Data* and the *European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* in all of which the right to privacy is a right of natural persons.

2. A cause of action for breach of privacy.

The Privacy Act should be amended to create a legal cause of action for breach of privacy.

2.1 A person whose privacy has been breached should be able to receive compensation as of right. Breaches of privacy may in some cases be corrected by changes in records about the person whose privacy has been breached. But if there has been publicity about a person's private affairs, especially where a person has

[1] For example the *Workplace Surveillance Act* 2005 (NSW).

suffered financial loss or the frustration of reasonable expectations as a consequence of the breach, a mere correction will not be able to right the wrong. For example, a person may have had a conviction quashed or charges dropped, yet an out of date record is retained and used, or is made accessible to others. No subsequent correction or apology can repair the damage.

2.2 The current system does not work well. First, it does not work quickly enough. It can take months for a complainant to get a hearing, and except in priority areas such as credit reporting, years to obtain a determination. By the time the Privacy Commissioner is able to deal with a breach on the Internet, the damage is done and those responsible may be long gone.

2.3 A major reason for the delay is that the Privacy Commission does not have sufficient funding to meet the demand. But there is never enough funding.

2.4 At present, a privacy complaint cannot deal with a situation where the taking of a person's particulars has made identity theft possible. We know of no definitive figures in Australia, but a study in the United States discovered hundreds of cases a year—cases where access was obtained to bank accounts, or where loans were taken out under borrowed names.

3. Requirements to make changes.

Of great importance is the ability of people to control their personal information. It should be possible to obtain an injunction from a tribunal, that changes must be made to a record or a web site, or that other breaches of privacy must cease, or that compensation is due.

3.1 The privacy act should also provide a means by which a person can prevent a threatened breach of privacy, or to reverse one that has occurred. That will include a right to prevent Government agencies from obtaining and retaining information that they are not entitled to, and to prevent dissemination of information that should be kept private.

3.2 The CCL does not have strong views as to what the tribunal should be. It could be that a division of the Australian Administrative Tribunal could specialise in privacy matters. Or there could be a separate privacy tribunal. Both would be more accessible than courts and may provide faster resolution of matters.

3.3 We suggest a two-tiered arrangement, as follows. An organisation should be able to opt in, and agree to be dealt with in accordance with a code, negotiated with the Privacy Commissioner. The act should include provision for penalties for subsequent failure to comply, and the option for persons whose privacy has been breached to receive compensation and correction accordingly.

3.4 Such an arrangement would enable an organisation, such as a small business, to have certainty about its obligations, and reduce the risk of meritless complaints. But if an organisation does not follow this path, it should be at risk that it will become the subject of privacy litigation.

3.5 It need not be the case that a breach automatically produces a penalty. The privacy tribunal might have the latitude to determine whether the breach was acceptable in the circumstances.

3.6 This approach should encourage even small businesses to treat privacy as a serious issue.

3.7 This policy should not be rejected on the basis of fears of litigiousness, of frivolous or meritless complaints. Consideration to the individuals who are harmed by breaches of privacy ought to override such concerns.

4. Remedies other than financial ones.

There needs to be a raft of remedies, including having information corrected, having misinformation and old information removed, having information for which the holder has no entitlement removed, having such changes passed on to those who have acquired material from the primary users, instead of or as well as financial compensation.

4.1 For example, a person who has a inappropriate photograph of them placed on the Internet without their consent should be able to have it removed, quickly without going to great legal expense.

4.2 A person should be able to protect their privacy by controlling what information can be passed to others, and what they do by way of passing that information to others. It is difficult, once information has been given to organisations in the private sector, to prevent it from being widely disseminated. The focus of current commonwealth privacy legislation is on the storage and dissemination of information. A better approach may be to regulate the entitlement to collect information as is the case in the NSW public sector[2].

4.3 This might involve a 'do not use my information' register, an extension of the 'do not call' register.

4.4 But once privacy has been lost, it can be hard, or impossible, to recover. New technology is particularly problematic. Fraudulent material can be published relatively anonymously on user operated sites such as *My Space*, for instance.

4.5 There is a need for quick action to be available, to prevent harm., such as the ability to secure a take down order against the operators of websites.

[2] S.8 *Privacy And Personal Information Protection Act* 1998 (NSW)

5. Intrusions

There should be a legal cause of action for intrusion.

5.1 So far, the Courts have been slow to find a legal cause of action for intrusion in the common law.

5.2 There is are a range of intrusions: surveillance by closed circuit TV, electronic tags of goods purchased which allow the shopkeeper to record what a person buys, radio frequency emitters embedded into consumables and stalking are some examples.

5.3 An example of misuse of closed circuit TV reported in a complaint to the NSWCCL occurred in a Strata Scheme block of units, in which cameras were placed by the owners' corporation on each floor and lobby of the building so members of the executive committee could watch who entered a unit. A unit owner was accused by members of the executive committee of being a prostitute because they observed that she was visited by a number of different men each night. Later, she was accused of drug dealing. In fact, she was a psychiatrist who accepted patients outside of business hours, and sometimes prescribed emergency drugs.

6. A general tort.

The new system needs to be based on principles that can continue to be applied as technology changes.

6.1 While adaptation will from time to time be necessary, it is desirable for the principles which define the tort to be general, so that the law can adapt to change.

6.2 An example of change which has caught up with the law is the steep reduction in the price of cameras. When the *Listening Devices Act* 1984 (NSW) was first passed, it was not necessary to have legislation to specifically cover surveillance, because cameras were too expensive for widespread use. Now short movies can be shot on cheap digital cameras, almost every mobile phone includes a camera, and we can expect hand-held devices to have more and more functions.

6.3 Again, the capacity to research a person through search engines on the internet by a person's name or other details and to then misuse the information that appears requires appropriate framing of the law. Similarly, placing private, possibly false, information on the Internet (in Wikipedia for example) so that it is accessible needs addressing.

6.4 Again, recent legislation[3] giving security agencies access to stored communications without warrant probably permits them to access, without warrant, people's bank accounts, since electronic versions of these are provided by the banks, and they remain unaccessed until an individual chooses to risk doing so. Bank customers have no choice about what details appear on their electronic account statements, and generally will be unaware of what details are there. Yet this

[3] Amendments to the *Telecommunications (Interception And Access) Act* 1979 including s. 6AA.

consequence of the legislation was not discussed when it was passed, and was probably not intended.

7. Emergencies and unintended consequences.

We accept that the legislation will need to allow exceptions to be made in order to provide protection of people in danger, and information to their relatives. Travellers should be asked in advance for permission for this to be done.

7.1 An example came from our work for Australian prisoners abroad. Despite the fact that lawyers were acting under instructions from the family of a prisoner, the Department of Foreign Affairs and Trade refused to provide information on the grounds that it was protected by the Privacy Act. This involved their misunderstanding of the application of Act, rather than an inability under the act to provide the requested information.

7.2 The circumstances of emergency, including the situations where, after a natural disaster, people want to know about the safety of their relatives, do need to be dealt with. One mechanism would be to add to the passenger departure form a box to tick declaring that the passenger is willing to have information released in such circumstances. This would also ensure that people who do not want their whereabouts released to indicate that.

7.3 That would also eliminate the need for a general exemption.

8. Young people and parents.

There is no automatic right of parents to know about the medical or educational problems of their children. This is an area where the law needs to be flexible, for the age of the child and the nature of the problem determine what is appropriate.

8.1 Most obviously, after a divorce where one of the parents is denied access to the child or young person because of child abuse, the provision of information to the abuser would be a breach of privacy.

8.2 Likewise, If a sixteen-year-old girl seeks information about contraception from a doctor, that is her business and no information or records should be provided to parents. Yet it may be crucial for a parent to know the diagnosis of a disease for a younger child. The law should err on the side of protection of privacy of the individual, including children, but provide mechanisms to allow it to be overturned.

8.3 A child of any age might reasonably expect that a temporary discipline problem at school is not automatically reported to the parents. But ongoing problems should be, since the school and the parents share responsibility for education.

8.4 Even then, confidentiality should be preserved. If a child cannot trust the school counsellor or a sympathetic teacher to maintain confidentiality, the child may not discuss a serious problem with anyone at all.

8.5 Giving a general entitlement to be informed to the parents eliminates the privacy of the child entirely. Depending on the case, there is a role for the child to be able to consent or to refuse consent to the parents being told. A separate serious of principles must be developed to deal with the privacy rights of minors due to the unique issues involved.

9 Exemptions for medical research

The norm for medical research should be that informed consent to publicity and to retention of personal details is required, just as it is for the research itself.

9.1 Institutional Research Ethics Committees (IECs) place their own requirements on medical research, and so does the National Health and Medical Research Council. Since it is condition of government research funding that IECs follow NHMRC guidelines, most do so, even when the research is not government funded. Nevertheless they can make mistakes.

9.2 For example, they can assume that the removal of names and individual identifiers will be sufficient to protect privacy. Yet in a recent case, a combination of general descriptions (an Australian state, ethnicity and sexual orientation) was enough to identify an individual, and to make his health details public.

9.3 IECs may also come to make exceptions where none is due. They have been known to allow research to proceed without informed consent because the subjects of the research would be worried if they knew they were part of an experiment. Informing them was deemed to be medically inadvisable, for no better reason than that. There have been other famous cases, like the Aukland Women's Hospital case[4], where ethics committees have scandalously failed in their obligations, including the obligation to require informed consent for a fatal experiment, let alone use of information.

9.4 In general, as part of the informed consent process, individuals should have the legal right to know what will happen to their information, and who will have access to it.

9.5 Where membership of social class is a relevant factor in medical research, it is conceded that requiring consent may bias the sample towards the bourgeoisie. It does not follow that the research requires a 100% sample. If the total population being studied is so large that obtaining informed consent is impossible, taking a modest sample, of say 5%, will generally be satisfactory. In the United Kingdom, longitudinal research is often done on samples of 1%.

9.6 Even where the notification of a disease is mandatory, and a 100% sample is therefore available, it is not often the case that the research needs all of it.

9.7 If informed consent for the use of information cannot be obtained from all the subjects of a piece of research, whether because it requires a very large sample or for

[4] Campbell, Alistair *A Report from New Zealand: an "unfortunate experiment"*, **Bioethics** Vol. 4, 1990

some other reason, the researcher should be required to seek special permission from the privacy tribunal if one is introduced, or from the Privacy Commissioner, in addition to the usual requirements of consent from an IEC following NHMRC guidelines.

9.8 There should be a place for patient organisations, such as the AIDS Councils, to have input into the responses to requests for release from privacy obligations.

10. Social science research.

Similar requirements should be placed on social science researchers. The reasons for privacy are even more cogent, because of the effects of their research upon minority and disadvantaged groups.[5]

10.1 Although social science researchers often argue that the NHMRC guidelines are stricter than is needed for their work, significant harms may result from it. Loss of privacy may expose subjects to scorn, contumely, victimisation, particularly in the case of faulty data matching. The research may also be destructive of relationships, involve deception, may develop or reinforce prejudices, or lead the participants to false views about themselves or others. Education research may result in the loss of competitive opportunities.

10.2 Research on groups may result in stereotyping, the creation of prejudice against the group, loss of privacy and dignity, affront, damage to the integrity of institutions, destruction of personal relations, and the destruction of inter-group relations.[6]

10.3 What becomes accepted in social science research impacts on the culture of research more generally. The impact on medical research culture in particular, is a further reason for not permitting lesser requirements for that research.

11. Exemptions for small businesses.

Small businesses may need special handling to avoid the imposition of unreasonable burdens. But that should not require a blanket exemption.

11.1 NSWCCL does not consider that small business should be exempt entirely from the provision of the privacy Act. There have been many examples of unacceptable infringement to individuals' privacy which we consider are unacceptable. However, we are also conscious that genuine small businesses have costs constraints which would make full compliance unworkable.

11.2 We support the maintenance of the exceptions to the exemptions for small business in circumstances where a small business provides health services, trades in

[5] The CCL has had discussions with the Australian Bureau of Statistics, in which we endeavoured to persuade them that they should not do research that involves 100% samples, when lesser samples would do as well.

[6] See for example the Code of Ethics of the Australian Association for Research in Education, in Martin Bibby (ed.) Ethics and Education Research, AARE 1997 pp. 116 & 120.

personal information, contracts with the Australian Government, is related to a larger business, is prescribed by regulation or elects to be treated as an organisation.

11.3 Whilst many small business may not pose a high risk to privacy, in an age where business of all sizes collect information electronically this assumption many no longer be entirely valid. Business of all sizes, even small ones hold databases of personal information of their clients, customers and suppliers etc. This includes financial information. Small business should not have an unfettered right, because of their size to use this information as they wish. For the period between 21 December 2001 to 31 January 2005, 20% of all NPP complaints to the OPC closed as outside its jurisdiction related to the small business exemption.[7]

11.4 We consider that there should be a code for small business which ensures that personal information is not abused. As a minimum the code should ensure that only relevant information is collected and that it is used in accordance with the purpose for which it was provided. Further that information should not be disclosed to third parties without the proper consent being granted by the owner of the information. Further, those dealing with small business should be advised that of the Code and should have a right, and be advised of their rights, to complain to the Privacy Commissioner in the event that they feel that their personal information was misused. If this complaint is upheld, there may be a series of sanction taken to remedy the situation from mandatory training about privacy and use of information or in serious abuses, the Attorney General using the power to prescribe a serious offender as being subject to the Act despite the exemption.

11.5 The Code may have other provisions that a relevant to certain types of small business but not others depending on the information that is collected and what use it is put to. Some of the provisions of the NPP may be adapted to small business. However, the Code should not be overly complex to maximise compliance by small business.

11.6 Related groups of business should not be able to benefit from the exemption by being broken up into small entities with annual turnover of less than three million where the total combined turnover is greater. This was raised as one concern in the ALRC Paper 31[8] Where companies are "related" in terms of the Corporation Law, they should also be so regarded for the purposes of Privacy Law and where combined turnover is greater than $3,000 000, the Privacy obligations should apply without exemption.

11.7 There should also be a tribunal that can deal with complaints involving small business that cannot be resolved by the OPC. This may be a separate division of the Administrative Appeals Tribunal. The Tribunal could, in the event that a complaint is upheld, impose monetary or non-monetary penalties, including orders for mandatory privacy law training. It can assess, whether in the circumstances of the case, the action of the small business is reasonable giving appropriate weight to the size and nature of the business.

[7] ALRC Issues Paper 31 p229.
[8] ALRC Issues Paper 31 p231

12. The exemption for political parties.

Subject to the constitutional right to freedom of political communication, political parties should be forced to comply.

12.1 In a digital age, political parties also hold considerable information about individuals and databases are substantial. This information is used for political campaigning and is part of the functioning of a modern representative democracy. However, there needs to be protection of what information is held, and importantly, how the information is utilised. The NSWCCL believes that political parties should comply with the Privacy Act. If an exemption applies at all it should do so only so far as is necessary to Political parties to check electoral rolls during election periods.

12.2 Individuals should be advised what information is being stored about them and for what purpose. In addition to being able to check the information that is held, individuals should be given the right to correct the information where it is inaccurate or incorrect. Such protections are made easier where, as is increasingly more common, communication is by electronic means. Individuals should be given some control over their personal information and should be able to easily withdraw their consent to information being held about them or used. Such measures would not, we believe, infringe the implied right of freedom of political information.

12.3 Political parties may be able to gather and store information about electors ethnicity or religion which may be misused. For example a Nazi style party storing information about electors religion.

13. The media.

Rather than there being a blanket exception, a code specific to the media should be developed, by which they should be bound.

13.1 Media organisations need to be free to collect and disseminate the news, current affairs and produce documentaries and the like. The public interest in having free press however, must be balanced against individual rights to privacy. A blanket exemption does not necessarily strike that balance and some measures to stem abuse by media organisations ought to be considered.

13.2 The exemption of the media applies to media organisations "in the course of journalism". A free press is also an important part of a functioning society. This phrase remains undefined, either in statute or by the courts.

13.3 NSW CCL is concerned that sometimes the media organisations go beyond what is reasonable and necessary in reporting news and current affairs with the aim being to scandalise and/or titillate and to increase sales at whatever cost.

13.4 We support the development of a Code for the media to ensure that unreasonable breaches of individual privacy are protected. This appears to be required to reign in unfettered harassment by "paparazzi" journalists. Such a code should establish accepted standards of conduct, as well as ensure that the publication of information is relevant to the communication being made and not merely scandalous in nature.

13.5 There should also be a mechanism whereby individual complaints can be lodged and dealt with by an independent body and the conduct complained of open to some scrutiny and redress where appropriate. There should be some effective sanctions to operate as a disincentive to abuse of the media's freedom to report. These may be of a monetary or non-monetary kind.

13.6 We also support the recommendation by the OPC Review that the Australian Broadcasting Authority be required to consult with the OPC when developing privacy codes for the industry and support greater involvement by the OPC in providing guidance and raising awareness of media organisation of privacy issues.

14. Privacy impact assessments.

Every parliamentary bill that affects human rights, including privacy, should require a human rights impact statement. This should occur, no matter how indirect the effect is.

14.1 A requirement that governments accompany proposed legislation with privacy impact statements is a good idea. But better would be a more general requirement, for a human rights impact statement, including the impact upon privacy.

14.2 The situation in New South Wales Parliament is a model of what not to do. Bills are often passed through both houses within hours of the press release, which is sometimes the first that the pubic hears of what is intended. In other cases, the Legislation Review Committee makes comments, but nothing is done. Or the concerns of members of parliament are assuaged by a section added to the bill requiring a review by the Ombudsman after a fixed period of time. The Ombudsman at the appointed time carries out a review (though he is not given enough resources to do an extensive job). makes a report—and no changes are made to the act.

14.3 Similar things are happening in the Federal Parliament. A good example is the sedition sections of the Criminal Code. The new sections were included in spite of the qualms of a number of members of the Government. Those qualms were assuaged with the promise that the ALRC would be invited to review the sections. The ALRC carried out a review, and made recommendations. And so far, apart from a brief dismissal of the review's findings by the Attorney-General, nothing has been done.

14.4 The *Telecommunications (Interception) Amendment Act* 2006 is a case in point. It introduced B-Party warrants, and there was a certain amount of public concern. There was no privacy impact statement. The Senate's Legal and Constitutional Committee was given so little time to debate it, they could only afford one day for hearings.

14.5 Still, a scrutiny committee, with representatives of all parties and the power to set its own timelines (with, say, an overall maximum), could ensure that the impact of new legislation on human rights, including privacy, received study and publicity. An advantage of a committee is that there are more likely to be minority reports. This can alert attention to problems, in a way that a single person could not.

14.6 Any member of such a committee should have the power to ensure that the committee examines a bill and reports to the parliament on its findings, before the bill goes through.

14.7 Better still would a situation where the reviews were carried out by an independent body, such as the Australian Privacy Foundation.

15. Credit reporting.

The only information that should be held by credit agencies is whether or not a person has defaulted on repayments. A lender will examine the borrower's current income and commitments. Nothing else is relevant.

The procedures of credit agencies and lenders should be strictly regulated, if necessary by a separate piece of legislation.

15.1 It is understandable that lenders and credit agencies should look for correlations between failure to keep up with debt repayments and other characteristics. It is their business to try to minimise risks, and to set interest rates according to those risks.

15.2 But correlations do not necessarily indicate a causal connection and are never enough to prove one. Where there is a causal connection, it may well be indirect. [9]

15.3 To conclude that because 62% of pointy-eared green people have defaulted on their commitments, that a new PEG applicant is a greater risk than the rest of the population, and therefore should be charged more, is to make an invalid deduction. It is, indeed, a form of prejudice. Acting on such prejudices is illegitimate discrimination, which may be illegal as well.

15.4 There is however widespread ignorance on such matters. The practice of credit agencies drawing conclusions from correlations which may well be *accidental* (not causally related) is already leading to discrimination. The more information that is kept, the worse that this problem is likely to be.

15.5 Arguments that there are benefits to those who would get cheaper loans because they are known "to have positive characteristics" should be resisted. For the cheaper loans are at the expense of those who are seen as being risks, having to pay higher rates. This is prejudice in practice.

15.6 Credit agencies misinterpret the data they do get. For example a person who shops around for the best terms is treated as though he or she had sought a loan and failed to get it. Their credit rating is affected, and so is what they have to pay.

[9] There was a correlation in the nineteenth century between the incomes of Scottish Presbyterian ministers and the price of whiskey. Both may be related to the general prosperity.

15.7 The invitation is also there for a credit agency to engage in illegal discrimination, say on the basis of race, in circumstances where it is not likely that the illegality will be discovered. Agencies that had access to genetic information would try and use it to discriminate.

15.8 If the *Anti-Money Laundering and Counter-Terrorism Financing Bill* 2006 is passed, a great deal of misinformation, including a great deal of speculation and guesswork, will be provided to government agencies. Such material should not inform any decision making, by any agency, government or private.

15.9 The more information that is kept, the more risk there is of mistakes. Residential tenancy databases provide a useful comparison. People are reluctant to supply information, or to take straightforward steps to settle their accounts, for fear of being blacklisted on a database. For being blacklisted leads to a person being made homeless.

15.10 For Example: A tenant had stained a carpet. At the end of his lease, he was reluctant for any of his bond to be used to pay for the damage. He was quite prepared to pay cash to rectify the damage. The reason was that he feared that if part of his rental bond were used, he would be listed as a default tenant who caused damage. His reluctance could lead to his being reported as difficult—yet it was based merely on a misunderstanding of the law.

15.11 There is a need, therefore, wherever personal information is held, for it to be accessible by the person, and for it to be quickly corrected if it is false or misleading.

15.12 We recommend therefore the procedures of credit agencies and lenders should be strictly regulated, if necessary by a separate piece of legislation.

16. Multiple use of data, and data matching.

There need to be multiple restrictions on the use of data which has been collected for one purpose, for another purpose. Such transfer should only be done with the knowledge and consent of the subject of the data.

16.1 Government departments and business organisations sometimes have many parts. At one stage, for instance, there was a Federal Department of Education, Employment and Youth Affairs. The transfer of data between Youth Affairs and Employment was as much a breach of privacy as transfer between the two separate departments was before the single department was created.

16.2 It is not enough, therefore, that information is restricted to the organisation that obtained it. Nor, in view of the intention to introduce the Access Card, will it be enough to ban information that is collected with one identifier from being linked to another.

16.3 A person may wish their medical record to be accessible to doctors in an emergency. That does not mean that they wish it all to be accessible to commissioner of taxation, or to Centrelink. There should be a legal cause of action for privacy

breaches where data collected for one purpose to be cross-referenced for another, without the subject of the information being told, and given the opportunity to resist.

16.4 In addition, those who collect data ought to be required to take reasonable steps to ensure that the data is accurate and correctly understood.

17. Privacy in the federal system.

The International Covenant on Civil and Political Rights gives the Commonwealth power to legislate to protect privacy. That power should be used, in the interests of consistency, and more importantly, to set high minimum standards.

17.1. The most important thing, in our view, that needs to be done federally is the introduction of legal cause of action for breach of privacy.

17.2 Any Commonwealth legislation however should not set out to be the whole of the law. Rather, states should be able to add their own protections, according to the circumstances and needs of the time.

17.3 A major problem at present is that there are too many gaps. Privacy is breached, and there is nothing that the victim can do about it. These issues should be addressed at all levels of government.