CIVIL ISSUES REGARDING THE PROTECTION OF PRIVACY

(WITH PARTICULAR FOCUS ON SUCH MATTERS AS AFFECTED BY THE INTERNET)

A. Laws and Regulations

1) What laws apply to protection of privacy issues in your legal system?

The principal piece of federal legislation regulating privacy in Australia is the Privacy Act 1988 (Cth). The Privacy Act regulates the handling of personal information by the Australian Government and the private sector. It contains a set of 11 Information Privacy Principles (IPPs) that apply to Australian Government and 10 National Privacy Principles (NPPs) that apply to the private sector.

Other federal legislation also regulates the handling of personal information. For example:

- the Freedom of Information Act 1982 (Cth) (FOI Act) provides that every person has a right of access to documents held by government agencies or ministers, other than exempt documents. A document is exempt from the freedom of information regime if its disclosure would involve unreasonable disclosure of ‘personal information’. This exemption is subject to an exception that a person cannot be denied access to a document on the basis that it contains his or her own personal information.

- the Archives Act 1983 (Cth) provides a similar exemption.

- the handling of tax file numbers (TFNs) is regulated under various federal Acts, including the Income Tax Assessment Act 1936 (Cth) and the Taxation Administration Act 1953 (Cth).

- the Data-matching Program (Assistance and Tax) Act 1990 (Cth) regulates data-matching using TFNs.

- the Census and Statistics Act 1905 (Cth) and the Commonwealth Electoral Act 1918 (Cth) require or authorise the collection of large amounts of personal information.

- Disclosure of personal information is also governed by the Australian Passports Act 2005 (Cth), Corporations Act 2001 (Cth), Telecommunications Act 1997 (Cth), Telecommunications (Interception and Access) Act 1979 (Cth) and Migration Act 1958 (Cth).

- Government agencies that obtain personal information are prevented by federal legislation from disclosing information that comes to them by virtue of their office other than in limited situations. Various acts of Parliament contain provisions that impose “secrecy” obligations on public servants.

Aside from the Federal legislation, each Australian state has its own legislative regime that regulates personal information and protects the privacy of individuals.
a) Public Sector provisions - are there civil code/legislative/common law provisions that protect individuals against privacy violations regarding:

- **Access by individuals to information collected by various government agencies about them**

  The *Freedom of Information Act 1982* (Cth) (FOI Act) provides that every person has a right of access to documents held by government agencies or ministers, other than exempt documents. A document is exempt from the freedom of information regime if its disclosure would involve unreasonable disclosure of ‘personal information’. This exemption is subject to an exception that a person cannot be denied access to a document on the basis that it contains his or her own personal information.

- **Protection from disclosure of that information to third parties**

  Most freedom of information laws provide for a “reverse-FOI” procedure that ensures that a third party to whom the information relates will be aware of the request and has an opportunity to express a view as to the disclosure of the information, and then to seek review of a decision to disclose.

  Under the Commonwealth FOI Act, an agency which receives a request for documents which contain personal information about a person, must not make a decision to grant access to that information unless the person to whom it relates has been given a reasonable opportunity to make submissions that the information is exempt under s 41 of the *FOI Act*.

  Personal information is defined in s 6(1) of the 1988 *FOI Act* as:

  > information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

  A number of submissions to the Senate Legal and Constitutional References Committee inquiry into the Privacy Act (the Senate Committee privacy inquiry) suggested that the definition of personal information in the Act needed to be updated to deal with new technologies and new methods of collecting information.


  In Victoria, the *Information Privacy Act 2000* (Vic) covers the handling of personal information (except health information) in the state public sector in Victoria, and by other bodies that are

---

1 ALRC Report, *For Your Information: Australian Privacy Law and Practice* (2008);
declared to be ‘organisations’ for the purposes of the Act. Organisations performing work for the Victorian government may also be subject to the Act, depending on their particular contract.

- Access by the media or members of the public to government records, for example, those regarding government decision-making and action, and limitations put on that access.

The Privacy Act contains a range of exemptions and exceptions. An exemption applies where a specified entity or a class of entity is not required to comply with any requirements in the Act. A partial exemption applies where a specified entity or a class of entity is required to comply with either: some, but not all, of the provisions of the Act; or some or all of the provisions of the Act, but only in relation to certain of its activities. An exception applies where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct.

Media organisations are exempt in relation to acts or practices in the course of journalism (section 7B(4) of the Privacy Act). A media organisation is an organisation whose activities consist of or include the collection, preparation and dissemination of news, current affairs, information or documentaries. Media organisations can claim the exemption if they have publicly committed to observing published, written standards that deal with privacy in the context of media activities. This exemption is intended to allow a free flow of information to the public through the media.

The FOI Act is described as an Act to give to members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies. Nevertheless, under the FOI Act the following classes/types of documents are exempt from the right to access:

- Documents affecting national security, defence or international relations;
- Documents affecting relations with States;
- Cabinet documents, unless officially disclosed;
- Executive Council documents, unless officially published;
- Internal working documents of an agency, a Minister, or of the Commonwealth Government where deemed contrary to the public interest, with certain exceptions;

3 Section 3 of the FOI Act 1982 (Cth) provides relevantly:

(1) The object of this Act is to extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth by:

   (a) making available to the public information about the operations of departments and public authorities and, in particular, ensuring that rules and practices affecting members of the public in their dealings with departments and public authorities are readily available to persons affected by those rules and practices; and
   
   (b) creating a general right of access to information in documentary form in the possession of Ministers, departments and public authorities, limited only by exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by departments and public authorities; and

(2) It is the intention of the Parliament that the provisions of this Act shall be interpreted so as to further the object set out in subsection (1) and that any discretions conferred by this Act shall be exercised as far as possible so as to facilitate and promote, promptly and at the lowest reasonable cost, the disclosure of information.
Documents affecting enforcement of law and protection of public safety;
Documents to which secrecy provisions of enactments apply;
Documents affecting financial or property interest of the Commonwealth, unless it is in the public interest;
Documents affecting certain operations of agencies;
Documents subject to legal professional privilege;
Documents relating to research by an agency;
Documents affecting national economy;
Electoral rolls and related documents.
This applies equally to the media and to members of the public.

- **Limitations put on information sharing between government agencies**

Information sharing between government agencies is limited by federal and State legislation, including:

- The Commonwealth public sector privacy scheme set up by the *Privacy Act 1988* (Cth) from 1 January 1989 applies to personal information held by federal public sector agencies. Privacy protection is defined by 11 Information Privacy Principles (IPPs).

- In Victoria, the Victorian public sector scheme set up by the *Information Privacy Act 2000* (Vic) applies to Victorian “public sector agencies”, defined to include universities set up by State legislation. This scheme began on 1 September 2001, with 10 Information Privacy Principles (VIPPs), but its full operation, including the ability to complain about breaches of privacy, commenced on 1 September 2002.

- Various federal and state regulatory bodies are subject to strict secrecy provisions regarding information collected on a person but those secrecy provisions contain exemptions enabling the sharing of private information with other specified regulatory bodies and government authorities in specified circumstances. Eg the Australian Taxation Office may share information with the Australian Crimes Commission, the Australian Securities and Investment Commission and law enforcement agencies.

- The *Data-matching Program (Assistance and Tax) Act 1990* (Cth), and guidelines issued under that Act,204 regulate data-matching using TFNs. Data-matching involves bringing together data from different sources and comparing them. Much of the data-matching done by Australian Government agencies subject to the *Privacy Act* is to identify people for further action or investigation for overpayment or fraud.

- There are also health privacy laws which apply to both the public and private sectors in the Australian Capital Territory, New South Wales (commencing in July 2004) and Victoria. Queensland, South Australia and Tasmania all regulate privacy through administrative arrangements within their public sectors. They have adopted principles based on either the Information Privacy Principles or National Privacy Principles from the *Privacy Act 1988* (Cth). The Northern Territory recently passed its *Information Act 2002* (NT) which includes privacy principles for the public sector. Both the Northern Territory and Western Australia are currently developing health-specific privacy legislation which is based on the proposed National Health Privacy Code. The net result is that there are dual regimes governing the handling of health records held by private sector health providers in the Australian Capital Territory, New South Wales and Victoria. At the same time, there is an incomplete coverage of public health records due to the absence of public sector privacy laws in some States.
The privacy schemes have similar structures. They protect various aspects of "personal information", defined in s 6(1) of the *Privacy Act 1988* (Cth) (on which all the other definitions are based) as:

- information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Most agencies with law enforcement functions are covered by the *Privacy Act 1988* (Cth), although a number of exceptions to the Information Privacy Principles (IPPs) exist for law enforcement activities. Two law enforcement agencies, however, are exempt specifically from the operation of the *Privacy Act*—namely, the Australian Crime Commission (ACC), and the Integrity Commissioner and staff members of the Australian Commission for Law Enforcement Integrity (ACLEI).

**b) Private sector provisions - are there civil code/legislative/common law provisions that protect individuals against privacy violations regarding:**

- Protection from disclosure to third parties of personal information collected in the world of e-commerce, for example
  - personal information provided through the use of credit/debit cards and other electronic transfers of funds;
  - personal information in relation to credit reporting and banking transactions;
  - records of a customer's usage (telephone; online activity);
  - records kept for insurance coverage and other social services benefits provided by the private sector?

Privacy provisions that regulate the handling of personal information in the private sector include:

- The Commonwealth private sector privacy scheme set up by the *Privacy Amendment (Private Sector) Act 2000* (Cth), which amended the *Privacy Act 1988* (Cth), extends to all non-government organisations except small businesses (with a turnover in the past financial year of less then $3 million), political parties, or State and Territory authorities.

- The Victorian health privacy system set up by the *Health Records Act 2001* (Vic) applies to organisations holding health records in Victoria whether public or private, with specific rules for health service providers, including hospitals. This scheme began operation on 1 July 2002, and contains 11 Health Privacy Principles (VHPPs).

The *Privacy Act 1988* (Cth) requires that agencies and organisations take reasonable steps to maintain the security of the personal information that they hold. This is commonly referred to as ‘data security’. The data security requirements for agencies and organisations are found in the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) respectively.

Compared to some other principles in the *Privacy Act*, the principles relating to use and disclosure in each of the IPPs and NPPs adopt a prescriptive approach. They do not contain an overriding qualifier, such as permitting use or disclosure where it is ‘reasonable’ in the

---

circumstances. The use and disclosure of personal information for the primary purpose for which it was collected is permissible. Other use and disclosure is prohibited unless it falls within the ambit of a specific legislative exception. The exceptions authorise, but do not require, a use or disclosure to be made. A note to NPP 2 provides that the principle does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.5

The IPPs and the NPPs both include a requirement to protect personal information from misuse and loss. These principles, however, differ subtly. As noted above, IPP 4(a) requires agencies to ensure that a record containing personal information is protected ‘by such security safeguards as is reasonable in the circumstances against unauthorised access, use, modification or disclosure and against other misuse’. An agency that does not take such steps will breach IPP 4, even if no loss, unauthorised access, use, modification or disclosure actually takes place.6 A number of Commonwealth documents also require agencies to adopt certain security measures. In particular, the Protective Security Manual (PSM) outlines minimum standards and procedures for Australian Government agencies, including requirements for: information security; personnel security; physical security; and tendering and contracting. Additionally, the Defence Signals Directorate (DSD) has published the Australian Government Information and Communications Technology Security Manual (ACSI 33), which sets out common principles for Commonwealth, State and Territory agencies to protect information held on information and communications systems.

NPP 4.1 requires an organisation to take ‘reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure’. The OPC has issued guidance on how organisations should meet this requirement, including through taking steps to implement:

• physical security, such as locks, alarm systems and access limitations;
• computer and network security, such as user passwords and auditing procedures;
• communications controls, such as encryption of data; and
• personnel security, such as staff training programs.

A number of national and international standards-developing bodies are presently working to develop standards on privacy and security issues, including Standards Australia and the International Standards Organization. In addition, the Australian federal government has created the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), in order to provide a secure forum for owners and operators of critical infrastructure; and government stakeholders to share information and discuss issues. The TISN was launched on 2 April 2003 in response to a recommendation of the Business-Government Task Force on Critical Infrastructure

---

5 Privacy Act 1988 (Cth) sch 3, NPP 2.1, Note 2.
which met throughout 2002.\textsuperscript{7} The establishment of TISN recognises the fact that about 90% of infrastructure is owned privately – hence the sharing of information between government and private agencies has become an important component of risk management.\textsuperscript{8}

- Protection from surreptitious collection of information via the internet, for example, through internet electronic surveillance technologies such as “spyware” or “adware”

The Privacy Act is intended to protect individual’s private information and, as such, its operation extends to information collected surreptitiously via the internet. However, this does not mean that protection offered is adequate, as the internet environment presents certain challenges that require special attention.

Currently, vast amounts of data are collected about internet users, often without their knowledge or consent. For example, data is often collected about the search terms an internet user has entered into an online search engine; the websites an internet user has visited; and the goods or services an internet user has purchased or inquired about online. Data is also collected about internet users who use tools provided by online search engines, such as free email and map services. These data have the potential to reveal a substantial amount of information about an internet user, including ‘information about health, education, credit history, [and] sexual or political orientation’. Information collected about internet users is not usually linked directly to an individual, but rather to a particular computer. This is because each computer connected to the internet is allocated a unique Internet Protocol (IP) address for the duration of each internet session.

Some information collected about internet users may be subject to the model Unified Privacy Principles (UPPs – now re-phrased to “Australian Privacy Principles”, see below). The UPPs were proposed by the Australian Law Reform Commission in its 2008 report, ‘For Your Information: Australian Privacy and Practice.’\textsuperscript{9} Modelled off the National Privacy Principles, the UPPs would be introduced into Australian legislation and would apply to governmental agencies and private organisations alike. However, whether or not the UPPs are introduced, a major issue with information collected electronically will remain - its permanency. For instance, in the context of deleting digital records, the Victorian Society for Computers and the Law has noted that:

\begin{quote}
[E]specially in the case of larger organisations, it may be practically impossible to guarantee the complete destruction of particular information, or if it is possible, the destruction process may be unreasonably costly and burdensome. The practical effect is that organisations requested to delete information may be encouraged to disregard such requests, to make only cursory and incomplete attempts to delete information, or to pass on the costs of deletion to consumers.\textsuperscript{10}
\end{quote}

The Internet Industry Association, of which many e-commerce companies are members, is one of

\begin{itemize}
\item Ibid.
\end{itemize}
the few industry bodies which are currently seeking approval for their own privacy code from the Commissioner. The draft Code was launched on August 16, 2001 by the Federal Attorney General, Daryl Williams AM QC and, having undergone public consultation, now awaits registration.11

**Update - The Australian Privacy Principles**12

Thirteen APPs will replace both the Information Privacy Principles (IPPs) (for the Commonwealth public sector) and the National Privacy Principles (NPPs) (for the private sector), although there are some areas where public and private sector obligations will differ. The collective term ‘entities’ has been introduced to cover both ‘agencies’ and ‘organisations’. The APPs appear to have more of a basis in the NPPs than the IPPs, with the effect that the changes will be more extensive for the public sector.

The APPs do not include a number of health-related provisions which may have been expected from their inclusion in the IPPs and NPPs. This is because the government is separately reviewing health privacy (and other areas referred to below) for later release. It is possible that consequential changes may be made to the APPs to reflect those other reviews.

As well as the APPs, the exposure draft includes some definitions and provisions relevant to the interpretation of the APPs.

The Australian Information Commissioner—a new position which will oversee the Privacy Commissioner from 1 November 2010—will be expected to issue issue guidance materials to assist entities to comply with the APPs.

---


2) What laws apply with respect to the investigation and enforcement of privacy rights?

The right to privacy is not a common law right in Australia, rather privacy is protected in a patchwork fashion by statute and certain causes of action such as trespass, nuisance, defamation and passing off, as well as the equitable doctrine of breach of confidence. The protection offered by the courts has expanded in recent times through the enforcement of obligations of confidence in respect of confidential information obtained in the absence of pre-existing relationship between the parties. However, the implementation of unified privacy principles that would apply nationally to allow investigation and enforcement of privacy rights, is yet to occur in Australia.

- How strong is the protection?

In the absence of a set of national, statutory, enforceable principles, the protection presently afforded is limited. The Australian Constitution does not provide for an explicit right to privacy, nor has such a right been implemented in any charter of rights, to date. The principal avenue of protection is therefore via the Privacy Commissioner’s, whose powers are limited to investigating alleged privacy breaches and attempting to settle the matters by conciliation (section 27 part 1 of the Privacy Act) – enforcement is effected through the Federal Court. As a result the protection in terms of privacy rights in Australia is not strong. This is so, despite the fact that increased attention has been devoted to legislative privacy provisions in recent years with the advent of the internet and related privacy issues.

- Are the laws binding or advisory?

The privacy principles ensconced in the Privacy Act are binding on those not already subject to a privacy code. However, due to the plethora of exceptions, much of the principles are advisory in practice and relying on industry self-regulation for compliance. In addition, as far as privacy codes are concerned, the Privacy Commissioner cannot initiate a code and cannot make a code binding on organisations that do not consent to be bound.

- How does an individual make a complaint when a private actor or government breaks privacy laws?

A complaint can be made in writing directly to the Privacy Commissioner (s.36(3) of the Privacy Act), or under an applicable privacy code. Alternatively, an individual may decide to take court action under one of the available causes of action such as trespass, nuisance, defamation and passing off, as well as the equitable doctrine of breach of confidence.

- Who prosecutes or enforces – for example, a privacy commissioner, administrative body, such as a privacy tribunal?

The Privacy Commissioner, under the Privacy Act, can make a formal determination as to whether a breach of privacy principles has occurred. Such a determination is enforceable through the Federal Court or the Federal Magistrates Court on application by either the Commissioner or the complainant. However, an aggrieved complainant has no right to have the merits of a Commissioner's determination under s 52 reviewed in court unless the respondent refuses to comply with a determination. Hence, the Privacy Act has been described by some as “light touch” legislation.

---

14 For instance, see Creation Records ltd v News Group Newspapers Ltd [1997] EMLR 444.
15 One exception to this was the case of Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637 (2005) 33 ABLR 45. There, court action commenced without the matter first being referred to the Privacy Commissioner. This was also the first case where the Federal Court analysed the National Privacy Principles (generally the Commissioner would provide guidelines on the principles).
16 Ian Turley, ‘Federal Court strengthens privacy enforcement: Seven Network (Operations) Limited v Media
• **Is there a right to a court remedy?**

There is not “right to privacy” as such, that would result in an automatic court remedy. Rather, as explained above, affected individuals may seek regr ess through a number of avenues, including trespass, nuisance, defamation and passing off, as well as the equitable doctrine of breach of confidence.

• **Are there out-of-court dispute resolution options?**

Yes. The primary avenue for this is the Privacy Commissioner, who has the power to settle matters through conciliation, under the *Privacy Act*. However, where an organisation is already bound by a privacy code that details the procedure for making complaints, the *Privacy Act* (s 36(1A)) explicitly precludes the making of a complaint to the Commissioner.

Depending on the parties involved, there may also be an option for mediation or arbitration.
B. Private-Sector Initiatives

1) Do particular companies, industries or professional associations in your country govern themselves regarding the protection of privacy? For example, are there privacy policies, professional codes, voluntary industry standards?

Legislation other than the Privacy Act allows for the development of privacy codes or rules. For example, s 112 of the Telecommunications Act enables bodies and associations in the telecommunications industry to develop industry codes relating to telecommunications activities. In 2000, the Australian Communications Industry Forum (now Communications Alliance Ltd) released an industry code on calling number display (CND). The Code requires suppliers to provide privacy protections in the supply of calling line identification (CLI) and CND; ensures that suppliers adopt procedures to allow callers to freely enable or block CND to the called party; require suppliers to inform their customers about CLI and CND and the privacy implications of both, and how customers can utilise CND blocking features.

Another example are codes developed pursuant to s 123 of the Broadcasting Services Act 1992 (Cth). Under this provision, the industry group responsible for representing various radio and television licensees (that is, commercial, subscription and community broadcasters) must develop a code of practice applicable to that section of the broadcasting industry. Privacy provisions are included in the various broadcasting codes of practice developed by representative industry bodies. In the commercial broadcasting and subscription broadcasting sectors, the privacy provisions relate to news and current affairs programs. In the case of the community broadcasting sector, the privacy provisions relate to all programs. For example, Code of Practice 2 of the Commercial Radio Australia Codes of Practice & Guidelines provides that news programs (including news flashes) broadcast by a licensee must not use material relating to a person’s personal or private affairs, or which invades an individual's privacy, unless there is a public interest in broadcasting such information.

In addition to legislative protection of personal information, organisations will often develop and publish privacy guidance that is not required by legislation. For example, the Australian Commission on Safety and Quality in Health Care is developing a National Patient Charter of Rights. The Charter will include a set of principles, including a principle dealing with privacy, which is intended to provide a consistent basis for the development of specific jurisdictional, disease and health service charters.

In addition, the private sector provisions of the Privacy Act exempt from its ambit acts by media organisations in the course of journalism when the organisation is publicly committed to observing a set of privacy standards.[168] The Australian Press Council (APC) has developed a set of eight privacy standards to regulate the handling of personal information. The Standards relate to the collection, use and disclosure of personal information; quality and security of personal information; anonymity of sources; correction, fairness and balance of media reports; sensitive personal information; and complaint handling. The APC receives and deals with complaints in relation to the Standards.

A number of approved privacy codes provide higher standards than those provided in the NPPs. For example, the Biometrics Institute Privacy Code provides a number of ‘Supplementary Biometrics Institute Privacy Principles’ relating to protection, control and accountability. There is no overlap with the NPPs, as a code replaces the NPPs for those organisations bound by it.
2) Who or what body, if any, ensures that these standards are met?

The Privacy Act 1988 (Cth) allows organisations and industries to have and to enforce their own privacy codes that continue to uphold the privacy rights of individuals while allowing some flexibility of application for organisations. Under Section 18BB the Commissioner may approve a privacy code, provided certain criteria are met. Before a code can be approved, however, the Privacy Act requires the Commissioner to be satisfied that:

- the obligations in the code are, overall, at least the equivalent of the NPPs; and
- the members of the public have been given an adequate opportunity to comment on a draft of the code.

If the code includes a complaints handling mechanism, the Commissioner must also be satisfied that the code:

- provides for a code adjudicator; and
- meets the prescribed standards and the Commissioner’s guidelines in relation to making and dealing with complaints.

Once a code has been approved, it will replace the National Privacy Principles under the Act for those organisations bound by the code. Codes must have a body established to oversee the operation of the code, called the code administrator. Each code administrator is required to keep a current record of code members, which are the organisations bound by the code.
C. International and Cross Border Issues

1) How is privacy protected when information is exchanged or transferred to other countries?

Section 5B of the Privacy Act applies the Act (and approved privacy codes) to acts done, or practices engaged in, outside Australia by an organisation, if the act or practice relates to personal information about an Australian citizen or permanent resident and either the organisation:

~ is linked to Australia by being a citizen; or a permanent resident; or an unincorporated association, trust, partnership or body corporate formed in Australia; or
~ carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.

Section 5B(4) extends the enforcement powers of the Privacy Commissioner to overseas complaints that fall within the criteria in s 5B(1). The purpose of s 5B is to stop organisations avoiding their obligations under the Act by transferring the handling of personal information to countries with lower privacy protection standards. The privacy laws of another country, however, will not be overridden by the Privacy Act. Where an act or practice is required by an applicable law of a foreign country, it will not be considered a breach of the Privacy Act.

Section 5B applies to organisations, but not to agencies. It is unclear whether, in the absence of an express statement, the Privacy Act operates extraterritorially in relation to the acts and practices of agencies. It could be argued that the IPPs apply to the records of Australian Government agencies wherever they may be.

The High Court has held, however, that in the absence of unambiguous language to the contrary, there is a common law presumption that courts do not read extraterritorial jurisdiction into legislation (Jumbunna Coal Mine NL v Victorian Coal Miners Association18). This presumption has been held to apply in the case of legislation that applies to agencies. There are a number of examples of federal legislation that regulates the Australian Government public sector and expressly provides that the legislation is to have extraterritorial application.

Update: proposed Australian Privacy Principles

Currently the Act extends to the offshore activities of private sector organisations in relation to Australian citizens and permanent residents. The exposure draft will extend this to apply to public sector agencies as well, and to protect all individuals, not just Australians.

APP 8 will regulate ‘cross-border disclosure’, where NPP 9 regulates ‘transborder data flows’. The government has sought to make it clear that:

~ there will be a cross-border disclosure where a third party offshore has access to personal information that remains in Australia, and

18 (1908) 6 CLR 309.
there will not be a cross-border disclosure where personal information is merely routed through servers outside Australia.

The new cross-border disclosure regime will mean that Australian entities that disclose personal information to third parties overseas will generally be liable for privacy breaches committed by those third parties—although the Australian entities may have recourse through their contracts. Some exceptions will apply—a number of which are consistent with those which currently apply under NPP 9. Notably, the exception relating to foreign laws and binding schemes will only require substantial similarity to the APPs ‘overall’. This relaxation of the requirement may go some way to opening up that exception for greater use by entities transferring personal information to other countries with robust privacy regimes.

2) Are there any agreements, laws or international treaties or protocols, to protect privacy issues in this situation?

The Preamble to the *Privacy Act* makes it clear that the legislation was intended to implement, at least in part, Australia’s obligations relating to privacy under the United Nations’ *International Covenant on Civil and Political Rights* (ICCPR) and the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines). The Second Reading Speech to the Privacy Bill also referred to the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, though this instrument does not bind Australia.

3) Does your country limit its exchange of information to countries with similar protections of privacy?

No. In this situation the onus is on the organisation to assess the regime of the country in which their trading partner resides. Many stakeholders, especially small businesses, have criticised the efficiency of this system arguing that they neither have the expertise or the resources to assess a foreign country’s privacy laws.  

---