THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000

EXPLANATORY MEMORANDUM

(Circulated by authority of the Attorney-General, the Honourable Daryl Williams AM QC MP)
This Bill is part of the Commonwealth Government’s commitment to enacting balanced privacy legislation for the private sector to ensure that full advantage may be taken of the opportunities that electronic commerce presents for Australian business within Australia and overseas.

The Australian public has expressed concern about doing business online, and this concern could frustrate the growth of electronic commerce. The Government acknowledges that user confidence in the way personal information is handled in the online environment will significantly influence consumer choices about whether to use electronic commerce. Any business demonstrating that it will protect the privacy of its customers will therefore gain a competitive advantage. Similarly, a country that can demonstrate it protects its citizens’ privacy will have an advantage over those countries that do not.

The Bill implements the National Principles for the Fair Handling of Personal Information (the National Principles), which were developed by the Privacy Commissioner following extensive consultation with business and consumers. The National Principles were intended to provide a basis for business to develop practices to ensure that the privacy of individuals was protected. They set out minimum standards in relation to how business and other private sector organisations should collect personal information, in relation to the use and disclosure of personal information and in relation to ensuring that the personal information they hold is accurate and secure.

The National Principles in the Bill provide a default framework for the protection of personal information. Private sector organisations will be bound by them, unless they have their own privacy code that has been approved by the Privacy Commissioner. A code will only be approved by the Privacy Commissioner if it provides at least as much privacy protection as the National Principles in the Bill.
Part IIIAA of the proposed legislation sets out the matters that the Privacy Commissioner must take into account when deciding whether or not to approve a privacy code. Where a code sets out a procedure for making and dealing with complaints, the Privacy Commissioner must consider the matters set out in sub-clause 18BB(3), including whether the procedures meet the prescribed standards. At this stage, the Government intends to prescribe the “Benchmarks for Industry-Based Customer Dispute Resolution Schemes” published by the Consumer Affairs Division of what was then known as the Department of Industry, Science and Tourism (August 1997).

The National Principles have been revised to accommodate legislative language and modified in their application to health information and transborder data flows. The modifications made to the National Principles in relation to health information are based on the Privacy Commissioner’s recommendations to the Government, following consultation with health stakeholders. The application of the National Principles to health information promotes a consistent, high level approach to privacy protection by organisations that hold health information, as well as other types of personal information.

**Application:**

The proposed private sector privacy legislation will apply to the acts and practices of “organisations”. An “organisation” is defined to mean a body corporate, an unincorporated association, a partnership, a trust and an individual. A body corporate that is related to another body corporate will be permitted to share information. However, related bodies corporate will be required to comply with the National Principles in the Bill in relation to using and handling the information. A similar rule exists in relation to the collection and disclosure of personal information by one partnership which dissolves to another partnership that forms immediately afterwards, has at least one partner in common with the first partnership and carries on the same (or similar) business as the first partnership.
The proposed legislation is not intended to cover the State and Territory public sector or State and Territory Government Business Enterprises (GBE’s) that perform substantially core government functions.
Extra-territorial operation of Act:

The Bill will apply to certain acts and practices of organisations which occur outside Australia. This is to ensure that, as far as practicable and appropriate, the legislation will apply in an environment where organisations operate across national boundaries and may move information overseas to use and process it. This is also intended to ensure that the provisions of the legislation are not avoided simply by moving personal information overseas.

Interaction with State and Territory legislation:

The Bill intends to establish a comprehensive national scheme providing for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by organisations in the private sector. State and Territory laws that make provision for the collection, holding, use, correction, disclosure or transfer of personal information will continue to operate to the extent that they are not inconsistent with the proposed Commonwealth legislation.

Application to the media:

The Bill includes an exemption for acts done and practices engaged in by media organisations “in the course of journalism”. This exemption seeks to balance the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media. The objects clause also highlights this need for a balanced approach.

A range of other provisions recognise the important role of the media in facilitating the free flow of information to the Australian public. For example, as part of the process of approving a code the Privacy Commissioner will have to be satisfied that code adjudicators will be required to have due regard to such issues. This is consistent with the obligation imposed on the Privacy Commissioner under existing paragraph 29(a).
In addition, the Bill provides that a journalist is not required to give information, answer a question or produce a document or record under the provisions of the Bill where this would tend to reveal the identity of a person who gave information to the journalist in confidence.

**Application to Employee Records:**

The Government has agreed that the handling of employee records is a matter better dealt with under workplace relations legislation. An act or practice engaged in by a current or former employer of a person in relation to an employee record will be exempt from the operation of the legislation if the act or practice is directly related to the current or former employment relationship. The requirement of a direct link to the employment relationship has been included to ensure that employers cannot use employee records for commercial purposes unrelated to the employment context.

An employee record is defined broadly as a record relating to the employment of an employee and includes the types of records typically held by employers on personnel files.

**Application to Small Business:**

All small businesses will be exempt from the operation of the legislation for a period of 12 months after the commencement of the legislation. This delayed application is designed to allow small business extra time to ensure compliance with the legislation. After the initial period it is intended that small business be exempt from the legislation unless there is a privacy risk. This is in accordance with Government policy to minimise compliance costs for small business.

A small business is defined as a business with an annual turnover of $3 million or less. Annual turnover may be calculated in the same manner required under the GST legislation. This is to ensure that the Bill does not impose a new obligation on small business.

A small business will be exempt from the operation of the legislation unless it:
• provides a health service and holds health information; or
• discloses personal information about another individual to anyone else for benefit, service or advantage; or
• provides a benefit, service or advantage to collect personal information about another individual from anyone else; or
• is a contracted service provider for a Commonwealth contract; or
• is prescribed by regulation.

Application to political parties and political representatives:

Political parties registered under Part XI of the Commonwealth Electoral Act 1918 will be exempt from the operation of the legislation. Acts and practices of political representatives such as members of Parliament and local government councillors (however described) will also be exempt from the legislation provided their acts and practices relate to an election, a referendum or other participation in the political process.

The acts and practices of contractors (and their sub-contractors) of registered political parties and political representatives will be exempt provided that the acts done or practices engaged in relate to an election, a referendum, or the participation of a registered political party or a political representative in the political process.

Acts done or practices engaged in by volunteers on behalf of and with the authority of a registered political party will also be exempt from the operation of the legislation.

Application where government services are outsourced to the private sector:

The Bill enables a contract between the Commonwealth agency and the contractor (and any subcontract) to be the primary source of a contracted service provider’s obligations in respect of the personal information collected or held for the purpose of performing the contract. Contractual clauses must be consistent with the privacy obligations that apply to the agency (generally, the Information Privacy Principles).
Contractors will be subject to the National Privacy Principles (or to an approved code) to the extent that they are not inconsistent with the Commonwealth contract.

A small business operator that is also a contracted service provider under a Commonwealth contract will be subject to the legislation in respect of the performance of the contract, but will be exempt in relation to its other acts and practices.

To ensure that people are able to find out what privacy standards apply, agencies and contractors will be required to release, on request, details of privacy clauses in their contracts.

As a safeguard, the Bill contains a provision explicitly prohibiting a contracted service provider from using or disclosing personal information collected under a Commonwealth contract for direct marketing purposes unless this is a necessary part of the contract itself.

Specific provisions will ensure that the complaints system works smoothly where the complaint is made about an act or practice of an organisation that is also a contracted service provider where that act or practice is in relation to a Commonwealth contract.

The Bill contains a provision to cover the situation where, for one of the reasons specified, a remedy cannot be obtained from a contracted service provider. It allows the Privacy Commissioner to substitute the agency for the contracted service provider and is intended to ensure that the agency remains ultimately responsible for the acts and practices of its contracted service providers.

Organisations providing services to a State government under contract:

A specific provision will exclude acts and practices of organisations performed in relation to a contract with a State or Territory instrumentality where that contract involves handling of personal information. Such acts and practices will not be covered by the Commonwealth’s privacy scheme but rather the State or Territory’s own privacy standards.

FINANCIAL IMPACT STATEMENT
The proposed amendments are expected to have no significant new financial impact on government. The Privacy Commissioner has been funded to administer the provisions that relate to the private sector. Private sector contractors that are providing services to the Commonwealth Government under contract, will be responsible for their own acts and practices that do not comply with the Bill. Any administrative costs for contractors of complying with privacy obligations may be taken into account when negotiating the contract price, so there will be no significant overall reduction in the Government's costs of complying with privacy obligations as a result of contracting out.

REGULATION IMPACT STATEMENT

The following information is provided in accordance with the Guidelines issued by the Office of Regulation Review, Productivity Commission.

INTRODUCTION

The development of electronic commerce is important for Australia’s future. Encouraging Australians to embrace the Information Age will maximise the potential benefits. The Government is looking to encourage business and consumer confidence by setting in place a legislative framework to support and encourage private sector led development of the information economy.

Buying and selling between individuals and businesses, banking and international trade in goods and services is increasingly being conducted over the Internet or through other information technology systems. The use of these new systems to conduct business transactions, purchase goods and services, pay bills or collect and retrieve information offers many benefits in terms of speed, convenience and records management.

However, the rapid developments in information technology, data networking and electronic commerce raise some correspondingly difficult economic and legal problems relating to taxation, security, privacy and jurisdictional issues.
Privacy has become a more significant concern as more people’s personal details are stored and exchanged as part of an electronic transaction. Common concerns centre on whether there is any protection for personal information, including how it is collected and stored, how it is used, whether it is secure and accurate, as well as whether an individual has a right of access to personal information held by an organisation about them. There are also concerns as to whether existing legal mechanisms are enforceable. Even if one country’s laws are adequate, it may be difficult to enforce rights under such laws as transactions may flow across many national borders, depending on where the business, consumer and website is located. For example, a single transaction can involve three or more countries making it hard to determine which country’s law will apply to the transaction.

The speed at which electronic commerce is evolving and changing makes it difficult for existing laws to be adapted. Any arrangements that are put in place need to provide an adequate and enforceable level of security and protection of personal information, while being flexible and technology-neutral so they can adjust to changing circumstances and emerging technologies.

At present, Australia has no comprehensive privacy laws applying to the private sector. Existing legislation includes the Privacy Act 1988 and the Telecommunications Act 1997. The Privacy Act applies to Commonwealth Government agencies, and to private organisations that handle credit information and tax file numbers (eg banks and credit unions). The Privacy Act sets standards for the collection, storage, use and disclosure of personal information. The provisions in the Telecommunications Act 1997 allow the Australian Communications Authority to request the development of an industry code dealing with privacy.

Since 1997-98, a self-regulatory framework has been operating in the private sector. The framework is based on the National Principles for the Fair Handling of Personal Information (the NPPs) developed by the Privacy Commissioner. These Principles reflect the Organisation for Economic Co-operation and Development (OECD) data protection principles. The purpose of the NPPs was to guide private sector businesses
in the development of practices for dealing with personal information that prevent its inappropriate collection, misuse, insecure storage or inappropriate disclosure. The NPPs also encourage organisations to be open about the personal information they hold and require organisations to provide an individual with access to personal information held about them.

Voluntary codes, based on the NPPs, have been developed in some industry sectors. The Australian Direct Marketing Association (ADMA) and the Insurance Council of Australia (ICA) have released codes based on the Privacy Commissioner’s NPPs, although the ICA’s code departs from the NPPs in certain respects. The Internet Industry Association has a draft code based on the NPPs. Other organisations, such as the Australian Retailers’ Association, are consulting with members on whether, and how, the NPPs might be implemented. The Australian Bankers’ Association has indicated that it favours a code that incorporates the NPPs through contractual agreements with customers. Other organisations have adopted internal codes, policies or standards, which may or may not be consistent with the Privacy Commissioner’s NPPs. Many industry sectors that regularly deal with personal information are partially covered by some form of regulation. Consequently, any move to more comprehensive controls over privacy will not impose onerous costs on the main affected industries.

The issues surrounding the protection of personal information, and the best strategy to secure such protection, have been publicly discussed for some time. Over the last two years, the Government has provided encouragement and assistance to business, through the Office of the Privacy Commissioner, to encourage the take-up of mechanisms to protect personal information held by them. However, the response from business has not been consistent and has not led to comprehensive personal data protection.

The Government’s election policy platform committed it to review the implementation of self-regulatory privacy protection in the private sector to ensure the fair handling of personal information by Australian businesses. The Attorney-General, through a core
consultative group, conducted this review. The Government’s decision to extend a privacy regime to the private sector is to be achieved by applying privacy principles, similar to those in the *Privacy Act 1988* that apply to the public sector, to personal information held by private sector organisations.

**ISSUES**

The extensive consultations over recent years on the absence of privacy protection in the private sector has raised a number of concerns that have not been resolved under the present self-regulatory approach. These include:

1. the potential for barriers to international trade for business;
2. the lack of protection afforded to the consumer;
3. the effects on the take-up of electronic commerce resulting from lack of protection to consumers;
4. the lack of comprehensive coverage of business;
5. the possibility that some States and Territories will impose stricter controls, which may result in inconsistencies between jurisdictions.

Businesses engaging in trade with European Union Member States are likely to experience difficulties under the current self-regulatory approach. There are serious questions surrounding the ability of Australia to meet the requirements for continued trade with EU Members under the *European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (“the EU Directive”). The need to meet the requirements of the Directive will result in ongoing costs to business associated with European Commission negotiations and will also affect the extent to which electronic commerce opportunities across borders can be fully utilised.

There is no indication so far that trade with non-EU Member States will be affected. This will depend on the extent to which other countries move to restrict transborder flows of personal information to countries that do not provide appropriate privacy safeguards. Various countries may consider such measures in order to satisfy the
requirements of the EU Directive. Some of Australia’s key trading partners are moving towards private sector privacy legislation. Canada currently has a private sector privacy bill before Parliament. The United States has a mix of legislative and self-regulatory protection. Several countries in our region have privacy legislation and others are understood to be considering the development of similar legislation. The extent to which a flow-on effect from the requirements of trading with EU Member States will result in other countries moving to restrict transborder data flows is not clear, but should not be discounted as a potential trade barrier in the future.

The lack of comprehensive protection of consumers’ personal information is an important element affecting consumer confidence in the information economy and, increasingly, participation in electronic commerce. Surveys conducted both here, and in other countries such as the United States, have indicated that consumer confidence in electronic commerce depends largely on the level of protection afforded to their personal information. Consumers want some limitations imposed on the private sector in respect of personal information which may be collected. Also, consumers want stronger controls regarding how their personal information may be used after it is collected and to whom it may be disclosed outside the organisation. The Government acknowledges that if this issue is not adequately addressed, it has the potential to hamper the growth of electronic commerce.

Notwithstanding the lengthy period of time during which consumer privacy has been recognised as a critical issue, particularly in the context of the growing information economy, the take-up of personal information protection by business has been variable and slower than expected. Codes or other means (for example, by way of contract) of implementing personal information protection already in place do not set consistent standards. For example, different codes nominate various dispute resolution bodies, creating jurisdictional problems and administrative burdens for business. In addition, no industry groups have 100 per cent coverage of their industry. In some cases, such as the ICA code, members are not bound unless they sign up to the code. For the protection of personal information to be effective, any voluntary scheme providing for this type of protection must be coherent and comprehensive in its application. This
has not occurred, in spite of the increased encouragement and support provided by the Government in the last two years.

The adoption of self-regulatory privacy codes by only some businesses has led to an absence of an effective and comprehensive data protection framework for the private sector in Australia. This has the potential to impact negatively on consumer and business adoption of electronic commerce and also Australia’s trading relationships.

However, the provision of any personal information protection imposes costs on business and it is important to take these compliance costs into account when developing a scheme for the fair handling of consumers’ personal information. The level of cost will depend on a number of factors, including:

- the flexibility of the regulatory approach adopted;
- the extent to which individual organisations are able to turn to recognised standards and mechanisms, or are required to develop them independently;
- the consistency of the standards to be applied across an organisation or industry sector; and
- the means of resolving disputes and the extent of redress that may be required.

The effectiveness of privacy protection for consumers will depend on the nature of the privacy scheme that is implemented. This includes the extent to which a scheme provides readily-understood, consistent levels of protection, affordable and accessible dispute resolution procedures, as well as the extent to which a scheme assists businesses to improve their practices, where necessary.
OBJECTIVES

The objective of the Government’s privacy policy is to reduce obstacles to the development, take-up and use of electronic commerce and other new technologies resulting from concerns about the possible mishandling of personal information by the private sector. In developing a system for the fair handling (collection, holding, use, disclosure and transfer) of personal information in the private sector the Government also aims to ensure that any scheme:

- is workable, consistent and cost-effective;
- provides Australian businesses with a framework which will assist them to take a leading role in the global information economy; and
- is compatible with the European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data to remove any potential barriers to international trade. (See Attachment A for a summary of the NPPs and relevant parts of the EU Directive.)

OPTIONS

There are a variety of possible options to address the problems identified. A regulatory strategy based on prescriptive Commonwealth legislation could be introduced. This option might involve the extension to the private sector of the framework that currently applies to the public sector under the Privacy Act. (The principles that govern the way the public sector should handle personal information are contained in s.14 of the Act, and are known as the “Information Privacy Principles” (IPPs). The standard they set for the public sector handling of personal information is slightly higher than that provided in the NPPs. The NPPs, whilst based on the IPPs, have been modified to take private sector business practices into account.) While having the advantage of providing a uniform approach applicable to all industries, professions, organisations, jurisdictions, activities and types of information, such a strategy could result in some inefficiencies. The legislation would not
necessarily provide any guidance to organisations on how the IPPs would apply in particular circumstances. As a result, compliance could impose considerable cost burdens on businesses, which may be passed on to consumers.

Other options involving minimal regulatory impact are available. These are self-regulation, which reflects the status quo, and co-regulation. The current self-regulatory system involves some industry-developed codes of practice without any legislative backing. Adoption of a code is voluntary and not necessarily uniform across a particular industry. There is, therefore, no way to ensure that all organisations in that particular part of the private sector adopt fair information handling practices.

Co-regulation would also foster industry developed codes, but these would be underpinned by legislation that would establish key principles and serve as a default framework in the absence of industry codes. As a general principle, most organisations in the private sector would be required to either adopt a code or comply with the legislative principles - either of which would require them to engage in fair information handling practices.

**OPTION ONE: SELF-REGULATION (STATUS QUO)**

The current, fully self-regulatory framework has a number of positive features. First, the ability of industry to develop codes leads to industry “ownership” which may foster a commitment to implementation greater than that which might apply under rules imposed through legislation. Second, codes are cost-effective, flexible, offer a large degree of sensitivity to market circumstances and are conducive to international competitiveness and product innovation. Australian businesses would be able to choose a level of privacy protection that allows them to compete internationally with foreign businesses.

As noted, some industries have already developed their own codes. However, the codes implemented to date have, in some industries, proved relatively ineffective because coverage is not comprehensive. For example, the Australian Direct Marketing Association’s (ADMA) code of practice for privacy protection covers only
organisations that are members of ADMA. It is obvious that non-member direct marketing organisations are not required to adhere to the principles found in that code.

Other industries have been reluctant to innovate in the area of privacy protection. For example, the final version of the Life Insurance Code of Practice did not address privacy issues. The life insurance industry was reluctant to take a position of leadership with respect to privacy protection, preferring to wait for direction from Government.

The major difficulty with self-regulation is that it may result in inconsistent standards across industries, and, as the system is voluntary, there is no way to guarantee that all organisations in the private sector will even adopt a code of practice. Where differences across industries are significant, problems may arise, particularly for organisations whose operations span a number of different industries. For example, the insurance industry may have to comply with codes drafted for life insurance, general insurance, finance, direct marketing and so on. A second potentially negative effect of self-regulation may be “regulatory arbitrage,” where organisations try to redefine their operations to fit within the most favourable code.

There may also be difficulties with enforcement. Self-regulatory codes do not usually provide consumers with any effective enforcement mechanism. The only means by which such codes could be made legally binding would be by inclusion by reference in a contract. Action under contract is cumbersome and costly for consumers and provides only limited remedies.

A central complaints mechanism, such as the Privacy Commissioner, would not be available to individuals under self-regulation. Where an organisation is required to comply with several different codes (which may conceivably have different enforcement mechanisms) a consumer may also have difficulty deciding how to commence an enforcement action in the first place. Ultimately, consumers may be reluctant to take any action if the cost and inconvenience of taking action is too high.

**OPTION TWO: CO-REGULATION**
The term “co-regulation” refers to a legislative framework within which self-regulatory codes of practice can be given official recognition. Legislation establishes the general principles with which all organisations must comply. It establishes the minimum benchmarks or safeguards that must apply across the board.

By providing the framework upon which industry codes are developed, the legislative approach ensures consistency and standardisation of personal information handling practices. In the absence of an industry code, the legislation would provide a default framework. The complaints mechanism available under the legislation would also provide a default mechanism where a code did not provide for a mechanism for consumers to make a complaint. The remedies available to the consumer under a code would be the same as those available under the legislation.

This option would appear to have significant advantages. First, it would ensure that all organisations would be required to adopt fair practices in relation to handling personal information, that there would be an identifiable mechanism for making a complaint about any organisation, and consistency and transparency in the remedies available to the consumer. Second, it would allow industries to develop codes tailored to the specific requirements of that industry. This would allow flexibility and sensitivity to industry and market needs. Third, industry would retain ownership of its code and its implementation process. Fourth, codes could be written in language readily understood by the operators in the industry, thus allowing their direct use at the operational level. Finally, the possibility of being able to amend codes would ensure that changing circumstances could be readily accommodated.

One difficulty with co-regulation, like the self regulation model, is that because codes may apply to acts or practices, or to certain information, or to a particular industry, there is a possibility that some organisations may have to comply with several different codes. Another difficulty may arise in relation to dealing with complaints. Organisations may have adopted a code that sets out a complaint resolution mechanism for consumers to use. Alternatively, complaints may be made to the Privacy Commissioner about an organisation where there is no code setting out a
complaint resolution mechanism which binds that organisation. The consumer may not always be aware of the relevant complaint mechanism and may become confused about where to go to resolve their problem.

**OPTION THREE: FULL REGULATION**

Full regulation would have the advantage of imposing a uniform framework across all Australian industries that collect, store and deal with personal information. Such a framework would not only implement general privacy principles, but would provide a uniform complaints resolution mechanism and ensure remedies available to the consumer (including compensation) were consistent across the entire private sector. It would also provide other countries with a more certain picture on how personal information was protected in Australia.

However, the extension to the private sector of principles enshrined in legislation would not recognise and accommodate specific industry requirements, and would not allow flexibility and sensitivity to industry and market needs. It would therefore entail high legal and compliance costs for government and business. These costs may eventually be passed on to the consumer and could potentially erode the competitiveness of Australian businesses competing internationally in a globalised online environment. It would also be difficult to adapt or amend legislation rapidly to accommodate changes in technology or commercial practices.

Full regulation is not an option that has been considered by the Government to date. However, if co-regulation does not work well it may be an option for the future. At present full regulation is not considered feasible and is not discussed in further detail in this RIS.

**IMPACTS**

**IMPACT GROUP IDENTIFICATION**

The groups affected by each of these options can be described as follows:
• the Commonwealth Government and its agencies (in particular the Federal Privacy Commissioner and the Attorney-General’s Department) as well as State and Territory Governments (‘government’);

• Australian businesses and other organisations in so far as they deal with the relevant forms of personal information (‘business’); and

• Australian consumers who deal with those businesses (‘consumers’).

The following analysis looks at the impact in terms of potential costs and benefits for the identified groups in respect of each of the options.

**ESTIMATING COSTS AND BENEFITS**

The Senate Legal and Constitutional References Committee in its March 1999 report on privacy issues noted that “costing of privacy schemes is difficult mostly because the variables are unknown. It is not easy to determine, for example, the extent to which consumers will complain, or the extent to which they will require compensation. Thus, administrative and other costs are difficult to predict.” A corresponding difficulty applies to the estimation of benefits, notwithstanding consumer surveys which indicate consumer confidence in electronic commerce is impeded by the absence of legal privacy protection in an on-line environment.

Witnesses giving evidence before the inquiry and parties making submissions in response to the Attorney-General’s Department’s discussion paper have been equally reluctant to make precise estimates of costs and benefits. In the *Information Privacy in Victoria* discussion paper it was noted that “the cost implications of the data protection regime will vary greatly from organisation to organisation. They will depend on the size and complexity of the organisation and its exposure to personal information.” For these reasons, this Regulation Impact Statement does not seek to give firm estimates in economic terms of impacts on identified groups, but assesses costs and benefits in more general terms on the basis of analysis and consultations.

What can be stated with confidence is that there are certainly legislative options available that do not impose unacceptable compliance costs, especially where these
legislative options, such as the proposed strategy, focus primarily on medium-sized and large businesses. The Victorian discussion paper cited a “survey conducted by Price Waterhouse in 1997, [which] revealed that major Australian businesses estimate that costs might not be significant. Of the 130 companies that responded, 79 per cent felt that only minor changes to their business practices would be necessary to comply with privacy legislation. Nearly two thirds of the companies, most with sales figures in the billions of dollars, believed it would cost them less than $100 000 to conform to any privacy legislation—less than 0.01 per cent of sales revenue.”

**OPTION ONE: SELF-REGULATION (STATUS QUO)**

**GOVERNMENT**

**Costs**

There would be no direct cost for the Commonwealth Government in continuing the current self-regulatory system apart from the costs associated with the Privacy Commissioner’s ongoing role in developing privacy protection in the private sector through assisting industries with voluntary codes (if the Government continued to support this role of the Privacy Commissioner).

Some State and Territory Governments may choose to proceed with legislation to protect privacy in the private sector. This may raise the overall cost to government of legislating through duplication of elements of the policy development and implementation process. The extent of these costs would depend on the strategies pursued by States and Territories choosing to legislate.

**Benefits**

Under self-regulation, the Commonwealth Government would not have to resource the development and implementation of a legislative regime for privacy protection in the private sector. It would also not need to resource the Privacy Commissioner to administer the NPPs and his increased powers and functions, including assisting with
the development of codes and providing a complaints and enforcement mechanism for individuals.

If State and Territory Governments chose to proceed with their own legislation this may provide some benefits from competition and innovation through the policy development process.

**BUSINESS**

**Costs**

First, under the status quo businesses will continue to face the costs of developing and implementing a self-regulatory framework for the protection of personal information. Businesses are only likely to invest in privacy protection if they perceive it as good business practice including some commercial advantage (eg, by acknowledging the statistical evidence which indicates that consumers value and seek privacy protection, especially in the electronic environment). It is likely therefore that within each industry there will continue to be a spread of businesses that offer different levels of privacy protection.

Businesses using electronic commerce (eg, to purchase supplies) that are interested in privacy protection may have to spend some time and money searching for businesses that offer the required level of protection. These costs are likely to fall over time for those businesses that tend to operate through established contacts. If businesses find search costs and the risks of using electronic commerce too high they may choose to use alternative services/payment methods. This may have some adverse effects on those businesses offering electronic commerce services (whether or not they have invested in privacy protection), from slower growth in demand.

For businesses using electronic commerce that have no concerns about privacy protection for individuals there will be no search costs.

A low level of consumer and market confidence in a purely self-regulatory framework may result in these businesses being unable to take full advantage of the benefits and
efficiency to be gained by utilising electronic commerce and other new technologies. This issue has been raised by a number of consulted parties, but no cost estimates are available.

Second, any State and Territory legislation in relation to private sector data protection may impose increased complexity and compliance costs on business as a result of having to adapt to varying State and Territory privacy laws. Overall, Australia’s existing legal frameworks are only limited in their coverage and vary widely across jurisdictions. A corresponding erosion of the international competitiveness of Australian businesses could also result. This concern has been raised in consultations but an estimate of the cost of complying with differential legislative frameworks has not been established.

Third, such an approach would not create a level playing field within Australia in terms of compliance with standards of protection for personal information. “Free riders” that do not provide effective protection could still benefit from the reputation of a sector that broadly does. Conversely, their behaviour could impact negatively on perceptions of organisations that comply in good faith. Compliant companies would also lose a direct competitive advantage over non-compliant companies, which do not assume the costs of compliance. The actions of organisations that do not provide effective protection could also undermine the credibility of data protection in the particular industry sector as a whole, creating a disincentive to invest in the development of self-regulatory protection. It may also provide a disincentive to consumers to embrace the services provided by that sector, as, for example, in relation to electronic commerce. The overall value of the potential damage caused by free riders is difficult to estimate.

Fourth, organisations that operate across multiple industry sectors may experience difficulties in complying with different standards under industry codes that operate in relation to different parts or activities of the one organisation. In addition, such organisations may experience extra burdens and costs involved in liaison and referral to various dispute resolution bodies established under different codes. On the basis of
extensive consultation, the Senate Legal and Constitutional References Committee reported that the costs of complying with multiple industry codes, often with different and even contradictory objectives, would probably be greater than the costs associated with a co-ordinated code-based approach underpinned by legislation.

Finally, in light of the information provided by the EC on their approach to ascertaining “adequacy” and the discussions between Australia, the EC and EU Member State officials, it appears unlikely that a purely self-regulatory approach will be regarded as adequate under the EU Directive. Business may continue to experience uncertainty regarding trade with the European Union. In addition, the EC has placed the hurdle somewhat higher in relation to self-regulation as opposed to legislative protection of personal information. The requirements regarding voluntary codes have been made more rigorous in order to address concerns about reduced enforceability and accountability. For example, it appears that the EC may require punitive sanctions to be available under voluntary codes but will not require similar sanctions to be available under a legislative scheme. It is difficult to estimate the value of the international trade that could be affected in this regard, but it has the potential to be significant given the EU is one of Australia’s major trading partners.

Industry associations in sectors with EU Directive compliant codes will incur the cost of ongoing negotiations with the EC in order to obtain an initial finding of adequacy, as well as ongoing liaison to satisfy the EC of continued adequacy. Businesses belonging to industries without EU Directive compliant codes are likely to incur the cost of ongoing individual negotiations with the EC in order to obtain and maintain a finding of adequacy. The cost of these private negotiations would depend on the extent to which Australian businesses were prepared to commit themselves to such negotiations in the absence of a legislative framework.

**Benefits**

Businesses that develop privacy protection regimes may attract additional business which could provide a competitive advantage for some firms. The extent of these
benefits will depend on how well informed consumers are, the nature of the privacy code and its effectiveness for those consumers who care about privacy protection.

Businesses will be able to decide for themselves whether to set up a scheme for the protection of personal information held by them, and if so, to what standard. They therefore have the ability to control the costs of implementing an industry or corporate code. Businesses that do not see a market advantage in self-regulating may choose not to do so, or choose not to enter into particular types of electronic commerce where the protection of personal information concerns are likely to be high. Self-regulation is probably more flexible and responsive to business and consumer preferences, and may be modified quickly and easily.

Also, Australian businesses could choose a level of privacy protection that would not erode their competitive position internationally to the same extent that a prescriptive, regulatory approach may. The exact value of these benefits would depend on the commercial decisions made by individual businesses, and has not been estimated.

Some private sector organisations, for example, the Insurance Council of Australia, that already have mature and comprehensive privacy protection standards, including a complaints resolution process, may prefer self-regulation to be retained. Self-regulation provides more scope for such businesses to tailor their consumer complaints mechanism.

**CONSUMERS**

**Costs**

The costs of self-regulation to consumers are derived from four main areas.

First, in a self-regulatory framework, consumers are subject to differing levels of protection for their personal information, depending on which organisation or sector they are dealing with. There may be confusion about requirements and the nature of any rights. The onus is placed on the consumer to investigate and evaluate their options regarding the levels of protection offered by particular organisations.
Second, due to geographic factors and/or the absence of protection for personal information across an entire industry, consumers will often have no choice but to deal with an organisation that offers no privacy protection. Where a code does apply, the ability of the consumer to enforce the obligations of a business in a particular industry will be limited by the availability and robustness of industry established and funded enforcement mechanisms. Consumers who deal with organisations or businesses that do not abide by a comprehensive self-regulatory code may be unable to obtain compensation or other redress, for example, to obtain correction of inaccurate information, or for loss or damage resulting from misuse of personal information. The cost of this lack of protection would depend on the kind and size of transactions undertaken and the extent of possible misuse of personal information.

Third, it is likely that those consumers dealing with companies that have developed and implemented information protection systems will pay the costs of those systems as absorbed into the prices of goods and services. Similarly, in the event of inconsistent legislation being passed by States and Territories, the cost of compliance with varying State and Territory privacy laws is likely to be passed on to consumers. The cost of goods and services, where they involve the transfer of personal information from Europe under the EU Directive, may be unevenly distributed. The precise extent to which these costs would be passed on to consumers would ultimately depend on commercial decisions of the affected businesses.

Fourth, the general Australian community would continue to have concerns about the way personal information is handled by Australian businesses in the on-line environment and may not have the confidence to avail themselves of the benefits of electronic commerce and other new commercial possibilities. The overall growth of the information economy in Australia could be stunted as a result, although there are no detailed costing projections in this respect.

Many potential misuses of personal information can impose a direct cost on the consumer. “Spam” email and direct marketing via bulk facsimile transmission are examples. If the transfer of an individual’s email address or fax number (along with
perhaps other information such as purchasing habits) results in that person receiving unsolicited communications, the nature of email and fax as a form of communication means that the cost of delivery will largely be borne by the recipient. This is also the case with the consumer’s cost in contacting the organisation to request no further communications. Australian businesses may be more likely to initiate such practices in a self-regulatory framework.

**Benefits**

Where consumers deal with an organisation that chooses to provide protection for personal information, they benefit from the privacy standards and enforcement mechanisms that the organisation voluntarily abides by. Conversely, consumers who are not concerned about the protection of personal information might choose to transact with an organisation that is not covered by a code, thus potentially taking economic advantage of any reduced costs under which that business may operate. Consumers may choose to take risks with their personal information in order to secure a cheaper product, although the precise value of this benefit to consumers is difficult to estimate.

Consumers may also benefit under self-regulation by not having to bear transferred compliance costs arising from prescriptive regulation. The value of these benefits would depend on commercial decisions and consumer behaviour.

**OPTION TWO: CO-REGULATION**

**GOVERNMENT**

**Costs**

The Privacy Commissioner, funded by the Commonwealth Government, will have a role in relation to:

- complaints resolution and general oversight of compliance for those businesses without privacy codes;
• evaluating, and deciding whether or not to approve, proposed privacy codes (the Privacy Commissioner would be required to consider many factors, and, before approving a code, would need to be satisfied that: the code sets out obligations that are at least equivalent to all the obligations set out in the NPPs; the code specifies the organisations that will be bound by it; that only organisations that consent to be bound by the code are, or will be, bound by the code; and that members of the public have been given an adequate opportunity to comment on a draft of the code. The code, if approved, would take effect on the day specified in the approval);

• supporting voluntary industry codes; and

• providing targeted assistance to businesses that hold little personal information.

Additional funding will be required for these functions. Further resources will also be required in the Attorney-General’s Department for the administration of the legislation. Indicative costs are $1.397 million in 1999/2000, with a total cost of $6.093 million over four years.

Benefits

The Government would be taking a role in the promotion of greater consumer confidence in on-line transactions with Australian businesses covered by the legislation and associated codes, and would thus be supporting the development of the information economy. It would also be providing some certainty to Australian businesses regarding trade with EU Member States, thereby facilitating international trade, with likely benefits for the wider economy. The precise economic value of these benefits would depend on a large number of variables.

The Government would also benefit from certainty about its compliance with privacy obligations where Government services are outsourced to the private sector.

Government would avoid some of the costs of a more prescriptive approach because the costs of developing industry codes, including dispute resolution, would be largely borne by business. The Privacy Commissioner would not be required to resolve
disputes relating to businesses that have their own approved privacy code consistent with the NPPs.

**BUSINESS**

**Costs**

Businesses will have to develop their own codes, including dispute resolution mechanisms, for the protection of personal information that comply with the NPPs and the other provisions in the legislation.

These compliance costs may include the cost of:

- the development of a privacy policy and procedure document and the advertisement of the policy and procedure in pamphlet form, and/or on the organisation’s website;

- reviewing the sort of information collected by the organisation and the way in which the organisation collects the information;

- reviewing the way the information is stored, and possibly developing a new and secure storage system for paper and electronic records in order to prevent unauthorised access to, or use or disclosure of, the information. This may involve the purchase of a secure facsimile machine, lockable filing cabinets, and/or a new computer system;

- reviewing the way in which the information is used and disclosed and modifying practices accordingly. This may involve the training of staff members about their obligations in relation to use of personal information and disclosure of that information. Identifying the types of organisations to which information is usually disclosed may lead to the redevelopment of forms and notices on websites.

This option may not impose the same level of additional costs on businesses that already provide privacy protection or have commenced adoption of a self-regulatory approach to privacy protection to the extent that some systems and training of staff would already be in place.
Those that currently offer protection for personal information or intend to develop their own privacy codes will incur few or no additional costs. If costs are incurred in upgrading or altering a code to fall into compliance with the legislation, these costs would depend on the nature of the existing code and the extent of the additional work that is necessary. There has been no precise estimate of the total cost across the private sector in this respect. Where a code already exists, and assuming that this code is commensurate with the NPPs established in the legislation, the additional costs for affected businesses should be negligible.

The impact of the proposed framework will vary across industry sectors. The importance of a strategy that is both uniform in its application of privacy principles and flexible enough to accommodate sectoral differences is illustrated by the case of the direct marketing industry. The direct marketing industry is, in a sense, based on trade in personal information. An implementation of a legislative framework without a recognition of the specific nature of the direct marketing industry could have a significant negative impact on this industry. The Australian Direct Marketing Association has sought to redraft its code of practice to take into account the Privacy Commissioner’s NPPs and has also actively examined different options for enforcement of its new code. Various provisions such as an “opt-out” capacity for consumers have been developed to satisfy the broad spirit of the NPPs. While the outcome of these efforts in relation to the proposed legislative framework is yet to be seen, the example of the direct marketing industry illustrates the capacity of the proposed strategy to operate uniformly, but with a degree of flexibility that can help to minimise negative economic impact on businesses.

Organisations that do not comply with personal information protection standards in an industry code may be required to provide compensation to consumers for harm suffered as a result of a breach of the code. If there is no relevant code, a breach of the legislation could also result in sanctions imposed by the Privacy Commissioner.

Co-regulation may be less flexible than full self-regulation. The capacity of Australian businesses to compete internationally with businesses that do not have the costs of
complying with such a framework may be somewhat diminished, and offshore businesses will continue to transact on-line with Australian consumers without being captured by a code or default privacy principles since they are likely to fall outside Australian jurisdiction.

The marginal cost of applying a privacy protection system, once implemented, to large amounts of information is probably relatively low. Costs are, however, potentially greater in relative terms for small businesses. To minimise compliance costs, it is proposed that small businesses be exempt from the operation of the legislation. Only those small businesses that pose a risk to the privacy of individuals will be made subject to the legislation. The treatment of small business under the legislation is explored in “Effects on Small Business” below.

Benefits

A legislative framework underpinning self-regulation would allow a continuation of the progress that has been made to date towards self-regulation, while correcting those elements that have acted to undermine effective privacy protection of personal information. Business will benefit in four main ways.

First, Australian businesses covered by the co-regulatory framework should benefit from increased consumer confidence in their systems for the handling of personal information. This will develop through the codification of privacy protection with legislative backing. The actions of organisations that do not voluntarily subscribe to any approved privacy code will be regulated by the legislative aspects of this scheme and therefore the organisations would find it more difficult to undermine the credibility and relative cost-effectiveness of privacy protection in the industry or sector as a whole. This approach would be likely to foster a level of consumer confidence in on-line transactions with Australian businesses, and should correspondingly increase the uptake of electronic commerce and new technology. Businesses will be able to take advantage of the savings to be made and the opportunities offered by utilising these new commercial platforms.
Second, Australian businesses will generally be able to operate on a level playing field domestically in terms of compliance with personal information protection standards. Organisations that choose to comply will no longer incur a cost disadvantage to “free riders” based in Australia. Organisations operating across multiple industry sectors will be less likely to be subject to inconsistent standards between codes that operate in different industry sectors, and would not be subject to the burdens and costs associated with liaison and referral to various dispute resolution bodies under different codes. The differential in commercial benefits for individual businesses between self-regulation and co-regulation with respect to compliance would vary depending on the difference in practical requirements for individual businesses between these two frameworks.

Third, a Commonwealth regulatory framework will provide national consistency for business and will remove compliance costs to business associated with varying or even conflicting State and Territory legislation. The benefits of the proposed co-regulatory framework, with its national uniformity, would outweigh any benefits from multiple State and Territory regimes. Significant cost advantages are to be derived from a single national privacy law. Electronic Frontiers Australia has noted that, “[a] major factor about not having a federal scheme, and possibly having many state schemes, is the cost of compliance. Under a federal scheme it would be one set of rules to follow. Under separate state schemes, one organisation operating nationally would be required to comply with seven different laws.”

Fourth, it would also be more likely to satisfy the requirements of the EU Directive and thus provide business with certainty in their dealings with European business partners. A uniform system representing international best practice has the advantage that there is no requirement to prove on a case by case basis that businesses comply with any particular privacy standards such as that for the EU. Mr Nigel Waters, a privacy advocate, has told the Senate Legal and Constitutional References Committee that, “even if some sectors or jurisdictions are able to pass the EU ‘adequate protection’ test, this would still leave most Australian businesses, and governments, in the situation of having to demonstrate on a case by case basis that they ensured
adequate protection for particular transfers or personal data from Europe. The cost, and cost of uncertainty, involved will potentially massively outweigh the modest compliance costs associated with a sensible, light handed statutory privacy scheme.” Under the proposed co-regulatory framework, the possibility that Australian trade could be adversely affected by the EU Directive would very likely be removed, although the total value of the affected trade, and the possible impact on this trade of variable outcomes from business level negotiations, has not been estimated.

**CONSUMERS**

**Costs**

Costs associated with implementing or upgrading an industry code, or complying with the default legislative framework, may be passed on to consumers. These costs may be transferred by affected businesses to the customers who benefit from these protection, or may be absorbed elsewhere. The monetary cost to consumers would depend on commercial decisions made by the affected businesses, and no precise estimate has been made.

Other costs to consumers may arise if opportunities for direct marketing are reduced. Consumers could receive less information about products and the range of goods and services available. The economic value of the decrease in information about products and services is, however, difficult to quantify.

There may also be initial costs for the consumer in seeking redress through dispute resolution procedures if an alleged interference with privacy is pursued by the consumer or a breach is established. For example, assuming the responsible business was within the jurisdiction of the amended *Privacy Act 1988* or an industry code, a consumer who has surrendered personal information to a number of different businesses would have to establish which business was responsible for the interference with privacy and the nature of the interference. There would also be costs involved in pursuing any possible breach whether through the Privacy Commissioner or the code mechanism. However, costs would vary from case to case.
Benefits

Consumers could more confidently use electronic commerce and other new technologies where these allow them to perform transactions with businesses covered by the legislation or an approved privacy code. They would therefore be more likely to enjoy the efficiencies and benefits of new technology. Consumer confidence in the existence of accessible and effective dispute resolution mechanisms, whether through the Privacy Commissioner in the legislation or in an approved privacy code, would develop.

There would also be consistency in the standards and therefore the level of privacy protection across all States and Territories, potentially reducing the compliance costs to business and the level of cost consequently passed on to consumers. Exact benefits would vary according to circumstances.

Community access to goods and services involving the transfer of personal information from EU countries would probably not be disrupted. The direct cost associated with unwanted “spam”, email and bulk faxes from direct marketing operations within the jurisdiction of the legislation or an approved code may also be reduced, as, under the proposed legislation, consumers would be given the opportunity to opt out of further direct marketing communications.
### Tabular Summary of Impact Analysis

<table>
<thead>
<tr>
<th>Cost and Benefits</th>
<th>Self-Regulation (Status Quo)</th>
<th>Co-Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost for Government</strong></td>
<td>Possible legislative duplication in different jurisdictions.</td>
<td>$1.397 million in 1999/2000, with a total cost of $6.093 million over four years.</td>
</tr>
<tr>
<td><strong>Cost for Business</strong></td>
<td>Cost of code development, framework duplication and conflict, possible diminished consumer and trading partner confidence. Cost of negotiations with EU.</td>
<td>Cost of code development, upgrade (minimised by legislative guidance), minor potential impact on international competitiveness, sanctions arising from breaches.</td>
</tr>
<tr>
<td><strong>Cost for Consumers</strong></td>
<td>Cost of code development may be passed on, potential lessening of confidence in Australian businesses.</td>
<td>Cost of code development may be passed on. Cost of seeking redress.</td>
</tr>
<tr>
<td><strong>Benefits for Government</strong></td>
<td>No additional Commonwealth funds.</td>
<td>Legislative duplication minimised.</td>
</tr>
<tr>
<td><strong>Benefits for Business</strong></td>
<td>Lower compliance cost, flexibility.</td>
<td>Savings resulting from guidance in code development. No framework duplication. Potential increase in consumer and trading partner confidence.</td>
</tr>
<tr>
<td><strong>Benefits for Consumers</strong></td>
<td>Possible lower prices.</td>
<td>Potential increase in confidence in Australian businesses.</td>
</tr>
<tr>
<td>Benefits likely to outweigh costs but does not deliver a comprehensive privacy scheme.</td>
<td>Benefits likely to outweigh costs and provides a more workable and nationally consistent privacy scheme than self-regulation.</td>
<td></td>
</tr>
</tbody>
</table>
EFFECTS ON SMALL BUSINESS

Before the legislation was introduced, it was considered necessary to identify categories of business, especially categories of small business (if any), or further categories of information (if any), that could be exempted on the ground that compliance costs would be unreasonable or excessive. Consultations between the Attorney-General, the Minister for Communications, Information Technology and the Arts, the Minister for Employment, Workplace Relations and Small Business, and officials from their Departments, sought to identify reasonable grounds for exemption. It was considered that, for some small businesses and organisations, the requirement to develop and comply with a code of practice, or the default provisions in the legislation itself, might not be justified in light of low privacy risk and potentially high compliance costs.

It was decided that small businesses would be exempt from the legislation unless they:

- provide a health service and hold health information; or
- disclose personal information about another individual to anyone else for benefit, service or advantage; or
- provide a benefit, service or advantage to collect personal information about another individual from anyone else; or
- are a contracted service provider for a Commonwealth contract; or
- are prescribed by regulation (regulations may be made to prescribe particular small businesses or particular acts or practices of small businesses to be subject to the operation of the legislation.)

Small business exemption criteria were originally suggested by the Office of Small Business. They were developed further in a paper written by the National Office for the Information Economy, with input from the Office of Small Business and the Attorney-General’s Department. One of the criteria for determining whether a business could be categorised as a “small business organisation” for the purposes of the Act refers to annual turnover. Annual turnover of $10 million was originally used...
by the Small Business Deregulation Taskforce. The Australian Taxation Office estimated that 93% of small businesses would fall into the exemption if the $10 million threshold was adopted, while statistics from the Australian Bureau of Statistics indicated that up to 85% of small businesses would be exempt from the application of the Act if the $10 million figure was used. Using the figure of $10 million was, however, identified as a possible problem in the paper prepared by the National Office for the Information Economy, because excluding such a high proportion of businesses was identified as having the potential to adversely affect the efficacy of the legislation.

The annual turnover figure of $3 million was finally adopted on the recommendation of the Department of Employment, Workplace Relations and Small Business. The Privacy Commissioner and the Attorney-General will review the figure from time to time to ensure that it remains appropriate.

The fact that small businesses may be exempt from the operation of the legislation because their annual turnover falls below $3 million and they satisfy the other criteria does not necessarily mean that small businesses can adopt practices that are contrary to the NPPs. Sound business practice and the possibility of falling outside the exemption where turnover exceeds $3 million will act as an incentive for small business to adopt general practices for handling personal information that are fair, while the exemption itself will reduce the administrative burden of compliance.

Small business, like other businesses, will be able to access whatever assistance and education is available generally through the Privacy Commissioner’s Office.

CONSULTATION

In recent years, there has been extensive public consideration of the need for privacy protection in the private sector, and the means by which it should be provided. There is ample evidence of the views of many business sectors, organisations and individuals on the options outlined above. Many individuals and organisations have made submissions in previous consultations by the Attorney-General’s Department, the Privacy Commissioner and various Parliamentary Committees. Where the views of a
particular sector or organisation are not known, it is unlikely, given the many opportunities that have arisen to date, that more formal consultation would elicit them.

Privacy and consumer advocates have for many years publicly lobbied the Government for protection for personal information through the enactment of legislation. More recently a number of key business players have approached the Government expressing their view in favour of a less prescriptive regulatory approach of the kind proposed. The Australian Chamber of Commerce and Industry, the Internet Industry Association and the Asia Pacific Smart Card Forum, which have previously supported a self-regulatory approach, have now advised that Commonwealth legislation, to underpin the application of approved self-regulatory codes, would be appropriate. The Credit Union Services Corporation has also advised of their support for Commonwealth legislation.

The Privacy Commissioner has been consulted and supports the proposal to provide a legislative framework to support and underpin approved voluntary codes.

In announcing the proposed legislation, the Government emphasised that it would be developed in consultation with business and privacy interests. The Government’s aim was to ensure that the legislation established sound privacy protection without placing unnecessary burdens on business.

Over 100 submissions received in response to the Attorney-General’s Department’s 1996 discussion paper, Privacy Protection in the Private Sector, have been considered in developing the policy. This was followed with the Department’s September 1999 Information Paper setting out the legislative framework and then the release of the key draft provisions in December 1999, which elicited more than 100 submissions.

There have also been submissions made to, and reports by, a number of Federal Parliamentary inquiries, including:

- the Joint Committee on Public Accounts and Audit Inquiry into Internet Commerce, which reported in June 1998 and recommended legislation to protect personal information held by the private sector;
• the Senate Select Committee on Information Technologies Inquiry into Self-Regulation in the Information and Communications Industries during 1998, which is yet to report; and

• the Senate Legal and Constitutional References Committee Report on Privacy and the Private Sector of March 1999, which recommended legislation in this area after examining evidence from well over 100 business, consumer and advocacy groups and individuals.

The Attorney-General’s Department has also considered a discussion paper released by the Victorian Government in 1998 (Information Privacy in Victoria) and Victoria’s Data Protection Bill drafted and released later that year. These sources have yielded valuable information on achieving privacy protection in the private sector.

Consistent with the aim of ensuring that one national regime is achieved, there has been wide consultation with the States and Territories. The States and Territories have taken the view that one national approach is desirable, and have assisted in the development of the Commonwealth legislation.

To facilitate consultation, the Attorney-General’s Department also established a Core Consultative Group (CCG) in 1999 including representatives from business, consumer and privacy groups, the Privacy Commissioner and the National Office for the Information Economy. The States and Territories were also represented. The business peak bodies represented a wide range of businesses with interests in the handling of personal information. Business, consumer and privacy interests were represented by:

Australian Chamber of Commerce and Industry
Council of Small Business Organisations of Australia
Australian Bankers’ Association
Investment and Financial Services Association

Credit Union Services Corporation
Insurance Council of Australia
Australian Finance Conference
Credit Reference
Real Estate Institute of Australia
Institute of Mercantile Agents
The State and Territory representatives were Multimedia Victoria, which represented officials supporting the Commonwealth-State On-Line Ministers’ Council, and the New South Wales Attorney-General’s Department, which represented officials supporting the Standing Committee of Commonwealth and State Attorneys-General (SCAG).

The CCG provided feedback on many issues and made a valuable contribution to the development of the proposed legislation. This formed a solid basis for an assessment of how the legislation might operate in practice and how various legislative approaches might impact upon business and be received by consumers.

Finally, the Attorney-General’s Department also published an information paper to solicit public comment, and convened a successful series of public consultation fora in Sydney, Melbourne and Perth in September 1999. The Department received submissions in response to the information paper from:

- Australian Dental Association
- Market Research Society of Australia
- Australian Institute of Credit Management
- Price Waterhouse Coopers
<table>
<thead>
<tr>
<th>Organization Name</th>
<th>Business or Organization Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Review Council</td>
<td>Cable &amp; Wireless Optus</td>
</tr>
<tr>
<td>People Living With HIV/AIDS</td>
<td>Commonwealth Bank of Australia</td>
</tr>
<tr>
<td>Australian Society of CPAs</td>
<td>Privacy New South Wales</td>
</tr>
<tr>
<td>Youth and Family Service (Logan City)</td>
<td>Australian National University</td>
</tr>
<tr>
<td>Australian and New Zealand College of Anaesthetists</td>
<td>Insurance Council of Australia Ltd</td>
</tr>
<tr>
<td>Law Institute of Victoria</td>
<td>Investment and Financial Services Association</td>
</tr>
<tr>
<td>Tenants’ Union of Queensland</td>
<td>Australian Competition &amp; Consumer Commission</td>
</tr>
<tr>
<td>Law Council of Australia</td>
<td>Public Interest Advocacy Centre</td>
</tr>
<tr>
<td>Australian Direct Marketing Association</td>
<td>National Australia Bank</td>
</tr>
<tr>
<td>Medibank Private</td>
<td>Australian Prudential Regulation Authority</td>
</tr>
<tr>
<td>Royal College of Nursing</td>
<td>Australian Finance Conference</td>
</tr>
<tr>
<td>Australian Council on Healthcare Standards</td>
<td>Australian Law Reform Commission</td>
</tr>
<tr>
<td>Department of Finance and Administration</td>
<td>Australian Communications Authority</td>
</tr>
<tr>
<td>Vonaldy Pty Ltd</td>
<td>Refugee Review Tribunal</td>
</tr>
<tr>
<td>Privacy Advocate</td>
<td>Southern Cross Broadcasting</td>
</tr>
<tr>
<td>Australian Chamber of Commerce and Industry</td>
<td>Australian Taxation Office</td>
</tr>
<tr>
<td>Australian Bankers Association</td>
<td>Federation of Australian Radio Broadcasters Ltd</td>
</tr>
<tr>
<td>Coles Myer Ltd</td>
<td>Australian Subscription Television and Radio Association</td>
</tr>
<tr>
<td>Australian Broadcasting Corporation</td>
<td>Australian Privacy Charter Council</td>
</tr>
<tr>
<td>Commonwealth Consumer Affairs Advisory Council</td>
<td>Special Broadcasting Service</td>
</tr>
<tr>
<td></td>
<td>Australian Press Council</td>
</tr>
</tbody>
</table>
During this extensive consultation process, key evidence and submissions from, for example, Price Waterhouse Coopers, the New South Wales Privacy Committee, the Australian Chamber of Commerce and Industry, the Internet Industry Association, the Asia Pacific Smart Card Forum, the Credit Union Services Corporation, the National Australia Bank and Telstra, have indicated broad support for the proposed strategy.

Price Waterhouse Coopers has supported a co-regulatory regime in the following words: “we agree that a co-regulatory approach, utilising Information Privacy Principles and the Codes of Practice is a suitable method to adopt. Self regulation methods are not enough to ensure compliance with the Act.” The New South Wales Privacy Committee is also committed to a co-regulatory approach to privacy in the private sector: “the co-regulatory approach suggested in the discussion paper is the Committee’s preferred option. This approach gives flexibility while retaining a safety net of minimum privacy standards.” The ACCI has noted that, “the strength of adopting a co-regulatory model, post a self-regulatory evaluation phase is that it represents evolution, not revolution.”

According to the Internet Industry Association, “Privacy concerns remain a significant impediment in the uptake of Internet usage, particularly for purposes of e-commerce. The [IIA] Code addresses this by fully implementing the National Principles for the Handling of Personal Information. We anticipate that private sector privacy legislation will be introduced this year by the Federal government.” Telstra has indicated that it is “desirable that there should be national privacy standards within a legislative framework.”

Of the options considered, public consideration has overwhelmingly favoured the proposed co-regulatory strategy. The CCG generally accepted most elements of the proposed co-regulatory strategy, including elements of codes; approval and revocation
of approved codes; giving effect to the NPPs in legislation and in codes; enforcement; public interest determinations; application of codes; the Privacy Commissioner’s role and functions; commencement and phase-in period; and elements relating to the acts and practices of employees.
The CCG generally accepted, among other things:

- the parameters for application of privacy codes;
- that a code should bind only a signatory or member of a signatory industry body;
- that a code should be based on the NPPs;
- that a code should set down a complaints handling process;
- that the Privacy Commissioner should approve codes;
- that the Privacy Commissioner should make available a public register of approved codes;
- that the default legislative framework should apply to an organisation that is not bound by an approved code;
- that determinations by the Privacy Commissioner should be enforceable in the Federal Court;
- that the Privacy Commissioner should be able to make public interest determinations that allow an organisation to do an act or engage in a practice that would otherwise be in breach of a Principle;
- that the Privacy Commissioner’s functions be expanded to investigate breaches of a code, approve and revoke codes, promote the NPPs, issue guidelines to help organisations to avoid breaches, issue guidelines for the development of codes, and provide advice on matters relevant to the Privacy Act;
- that there be a phase-in period during which the Privacy Commissioner’s functions would be extended, codes would be developed and augmented to meet legislative requirements, and education, advice and guidance programs would be implemented;
- that the balance of the provisions would come into effect after a further twelve months or on 1 July 2001, whichever is later; and
• that, under certain conditions, anything done by a person in the performance of
their duties as an employee is treated as if done by the employer organisation.

These issues were considered by the CCG in great detail.

CONCLUSION AND RECOMMENDED OPTION

It is proposed that introducing legislation under Option Two would meet the specified
objectives of achieving a workable, consistent and effective scheme of personal
information protection in the private sector and would foster business and consumer
confidence in, and thereby increase the take-up of, electronic commerce and other new
technologies. It would provide at least cost:

• a privacy protection framework which will assist business in taking a leading
role in the global information economy;

• coherence in setting a national standard set of principles, thereby simplifying
issues for organisations which operate across industry sectors;

• a single comprehensive framework so that businesses are not faced with the
prospect of inconsistent State and Territory legislation; and

• certainty regarding trade with European Union Member States.

Considering the costs and benefits, Option Two is recommended. Experience in the
development, implementation and operation of a self-regulatory approach to date has
demonstrated that Option One is unlikely to meet policy objectives in the near future.
Option Three is considered too expensive and inflexible for government and industry.

IMPLEMENTATION AND REVIEW

The Attorney-General will be responsible for administering the Act. The
Attorney-General’s Department will be responsible for the ongoing monitoring of its
operation. Currently the Privacy Commissioner is able to report to the
Attorney-General on privacy issues and reports annually on the Privacy Act 1988. The
Privacy Commissioner’s reporting functions will be extended to cover the protection
of personal information in the private sector, including the operation of the proposed
legislation. Under the Competition Principles Agreement, a comprehensive review of any Commonwealth legislation enacted to underpin self-regulation will be required within ten years of its implementation. It is likely that this legislation will be reviewed by the Privacy Commissioner in two years time, especially in relation to the operation of the exemptions.

ATTACHMENT A

1. NATIONAL PRIVACY PRINCIPLES:

There are ten National Privacy Principles, which are summarised below:

NPP 1 relates to the collection of personal information by an organisation. An organisation must only collect personal information where it is relevant to one or more of its functions or activities, and the way it is collected must be fair. The organisation should, where possible, collect the information directly from the individual concerned. At the time of collection, the organisation should tell the individual who it usually discloses the information to.

NPP 2 governs how an organisation may use and disclose personal information in its possession. There are restrictions on the way in which an organisation may use or disclose personal information where that use or disclosure is for a purpose other than the primary purpose for which it was collected.

NPP 3 relates to the quality of the data held by an organisation. An organisation must take reasonable steps to make sure that the personal information it holds is accurate, complete and up-to-date.

NPP 4 states that an organisation must take reasonable steps to make sure the personal information it holds is secure, and destroy or de-identify personal information if it is no longer needed for any purpose.
NPP 5 requires an organisation to be open about what personal information it holds and its policy on its management of personal information.

NPP 6 relates to access to, and correction of, personal information held by an organisation about an individual, by that individual. The general rule is that an organisation should let an individual have access to the personal information held about that individual. There are, however, exceptions to this general rule. An organisation should correct information held about an individual where that individual is able to establish that the information is not accurate, complete and up-to-date.

NPP 7 regulates the use of identifiers assigned by a Commonwealth agency.

NPP 8 states that individuals must have the option of not identifying themselves when entering transactions with organisations, if it is lawful and practicable to remain anonymous.

NPP 9 regulates the transfer of personal information held by an organisation in Australia about an individual to someone (other than the organisation or the individual) in a foreign country.

NPP 10 places limits on when an organisation is permitted to collect sensitive information (ie, information or an opinion about an individual’s racial or ethical origin, political opinions, religious or philosophical beliefs, political or religious affiliations, membership of a trade or professional or union, sexual preferences or practices, criminal record, or health information.)

2. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA:

CHAPTER II: general rules on the lawfulness of the processing of personal data
Article 6 relates to the fair processing of personal data. “Processing” is defined as any operation or set of operations performed on personal data including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. The article requires that information that is collected be collected for a particular purpose and used in a way that is compatible with that purpose (this is incorporated in NPPs 1 and 2); that information be accurate, complete and up to date (this is reflected in NPPs 3 and 6), and be kept in a form which permits the identification of data subjects for no longer than is necessary (addressed in NPP 4).

Article 7 lists the criteria for making data processing legitimate, namely, consent from the data subject; or the necessity to process the information for -

- the performance of a contract to which the data subject is a party;
- compliance with a legal obligation; or
- to protect the vital interest of the data subject; or
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller of the data or a third party to whom the data was disclosed; or
- the purposes of the legitimate interests pursued by the controller or by a third party to parties to whom the information is disclosed.

(NPP 2 incorporates similar limitations on the use and disclosure of personal information).

Article 8 regulates the processing of “special categories” of data (the same sort of information covered in the definition of “sensitive information”, to which NPP 10 applies).

Article 9 requires that Member States shall provide for exemptions for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or
literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. (This matter is not covered in the NPPs, but by amendments to the existing Privacy Act. The Privacy Commissioner will, in exercising his or her functions under the Act, be required to consider the desirability of the free flow of information through the media or otherwise. Generally speaking, acts done, or practices engaged in, by an organisation will be exempt from the operation of the Act if the acts are done, or the practices are engaged in, by the organisation in the course of journalism.)

Article 10 relates to the information that a collector must tell the individual, where the collector gets the information directly from that individual. The collector must provide to the individual (the “data subject”) information about the identity of the controller, the purposes of the processing for which the information is intended and further information, such as who will receive the data, whether replies to questions are mandatory and the consequences of failing to provide information, and the existence of the right of access to and the right to rectify data concerning him or her (NPP 1.3 requires organisations to inform individuals of these things.)

Article 11 requires the controller of data that has not been collected directly from the data subject to provide the data subject with information about the controller’s identity (and other information, as identified in Article 10), except where the provision of such information proves impossible or would involve a disproportionate effort (this situation is addressed in NPPs 1.3 and 1.5).

Article 12 requires Member States to guarantee every data subject the right to obtain from the controller, whether or not the controller has data about the subject, and if so, for what purpose and who it will be disclosed to and what data the controller holds about the subject (this is addressed in NPP 6). Article 12 also requires the controller to rectify, erase or block data where the processing does not comply with the provisions of the directive because the information is inaccurate or incomplete. (NPP 4.2 requires an organisation to destroy or de-identify information no longer needed for any purpose.)
Article 13 outlines circumstances in which it may be appropriate to restrict the scope of the obligations and rights provided for in Articles 6(1) (which relates to collection and quality of data), 10 (which relates to the procedure for collection of information directly from the data subject), 11(1) (which relates to the procedure where information is collected from sources other than the data subject), 12 (which relates to the data subject’s right to know what information is held about him or her by the controller) and 21 (which relates to the processing of publishing operations). These circumstances (including measures to safeguard national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences; an important economic or financial interest of a Member State etc) have been taken into account in drafting the NPPs, most notably NPP 6 (in relation to an individual’s right of access to personal information held by an organisation about that individual).

Article 14 provides that Member States shall grant the data subject the right to object to the processing of information about him or her, particularly where the information is to be used or disclosed for the purpose of direct marketing. NPP 2.1(c) expressly gives the individual the right to opt out of receiving further direct marketing communications from a particular organisation.

Article 15 provides that Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or her, or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her (such as performance at work, creditworthiness, reliability, conduct etc).

Article 16 provides that any person acting under the authority of the controller or processor of personal data must not process the data except on instructions from the controller (unless he or she is required to do so by law).

Article 17 requires Member States to ensure that the controller of personal data has appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access (this matter is addressed in NPP 4). Where processing is carried out on the controller’s behalf, the
controller must choose a processor that provides sufficient technical security measures, and ensure compliance with those measures. The carrying out of processing on the controller’s behalf must be governed by contract or legal act binding the processor to the controller, and requiring the processor to conform to the obligations imposed on the controller to provide appropriate security for the data.

Article 18 provides that Member States shall provide that the controller of information must notify the supervisory authority (described in Article 28 as an independent public authority responsible for monitoring the application of the provisions adopted by the Member States) before carrying out any wholly or partly automatic processing operation (or set of operations) intended to serve a single purpose or several related purposes. The article also provides for simplification of the notification process or exemption from the process altogether, in certain circumstances. Article 19 sets out the information to be given in the notification.

Article 20 requires Member States to determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and to check (itself or through a supervisory authority) that the processing operations are examined prior to the start thereof.

Article 21 requires Member States to take measures to ensure that processing operations are publicised, and that a register of processing operations be kept by the supervisory authority, and may be inspected by any person.

CHAPTER IV: transfer of personal data to third countries:

Article 25 requires Member States to ensure that the transfer of personal data to a third country (for processing) may only take place if the third country ensures an adequate level of protection, and outlines the procedures for assessing whether protection is adequate, and for dealing with the situation where a third country does not ensure adequate levels of protection. Article 26 sets out the circumstances in which the
transfer of personal information is allowed to a third country that does not ensure an adequate level of protection. NPP 9 requires similar safeguards where personal information is transferred to a foreign country.
NOTES ON CLAUSES

Clause 1. Short title

This clause is a formal provision that provides for the Bill, when enacted, to be cited as the *Privacy Amendment (Private Sector) Act 2000*.

Clause 2. Commencement

2. This clause provides that the Bill, when enacted, will come into operation on the day 12 months after the Bill receives Royal Assent, or 1 July 2001, whichever is later.

Clause 3. Objects

3. This clause sets out the broad policy aims of the amendments contained in this Bill. The main object of the Bill is to establish a comprehensive national privacy scheme for private sector organisations and to do so in a way that meets international concerns and Australia’s international obligations relating to privacy recognising, in particular, individuals’ interests in protecting their privacy. The clause also recognises that there are important human rights and social interests which compete with privacy, such as the desirability of the free flow of information to the Australian public through the media and otherwise.

Clause 4. Schedule(s)

4. The provisions in the *Privacy Act 1988* (hereafter called the Act) are amended or repealed as set out in Schedule 1 of the Bill. Schedule 2 contains amendments to other Acts, and Schedule 3 contains amendments in relation to disclosures to intelligence bodies (the Australian Security Intelligence Organisation and the Australian Secret Intelligence Service).
SCHEDULE 1 - AMENDMENT OF THE PRIVACY ACT 1988

Item 1. At the end of section 3

5. Item 1 amends existing section 3. While the Bill intends to establish a comprehensive national scheme providing for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by organisations in the private sector, State and Territory laws that make provision for the collection, holding, use, correction, disclosure or transfer of personal information will continue to operate to the extent that they are not inconsistent with the proposed Commonwealth legislation.

Item 2. At the end of section 3

6. Item 2 adds a note at the end of section 3 confirming that State and Territory laws will continue to have effect in relation to the interpretation and application of the National Privacy Principles.

Item 3. At the end of Part 1

7. Item 3 adds a new clause 5B to the Act. New clause 5B describes the extra-territorial operation of the Act. The Act will apply to certain acts and practices of organisations which occur outside Australia. This is to ensure that, as far as practicable and appropriate, the legislation applies in an environment where organisations operate across national boundaries and may move information overseas to use and process it.

8. This provision is also intended to ensure that the provisions of the legislation are not avoided simply by moving personal information overseas. The Act will only apply to acts and practices outside Australia in relation to personal information about Australian citizens or those people whose continued presence in Australia is not subject to a limitation as to time imposed by law. Clause 5B draws a distinction between organisations which have a significant organisational link with Australia and organisations which do not have such an organisational link with Australia but which,
nevertheless, carry on business in Australia.
9. Sub-clause 5B(2) sets out those organisations which have a significant organisational link with Australia, for example, a partnership formed in Australia, a trust created in Australia, a body corporate incorporated in Australia or an unincorporated association that has its central management and control in Australia. Where such organisations deal with the personal information of Australians, the Act will apply to all acts and practices outside Australia.

10. Sub-clause 5B(3) deals with organisations that do not have this kind of link with Australia, for example, a foreign corporation. Where these other organisations carry on business in Australia and deal with the personal information of Australians, the Act will apply to acts and practices which occur outside Australia where the organisation collects or holds the personal information in Australia. This is to ensure, for example, that where the personal information of Australians is collected in Australia by a foreign organisation doing business in Australia, the information will be handled appropriately whether it is held by the organisation in Australia or overseas. Where a foreign organisation collects personal information about Australians outside Australia, the Act will only apply if the information is transferred into Australia. Once the information is held in Australia, the Act will apply to acts and practices outside Australia in relation to that information.

11. Where a foreign organisation collects personal information about Australians overseas and holds that information overseas, the Act will not apply except to the extent that National Privacy Principle 9 applies to the transfer of personal information to that organisation from an organisation in Australia.

12. Sub-clause 5B(4) will allow the Privacy Commissioner to take action overseas in relation to complaints received about acts and practices which occur overseas. Sub-clause 5B(1) provides that approved privacy codes apply in relation to acts and practices which occur overseas. In drawing up codes of practice which provide for complaint procedures, organisations will need to consider the powers of code adjudicators in relation to investigating acts and practices which occur overseas.
Item 4.  Subsection 6(1) (definition of *annual turnover*)

13. Item 4 refers to the definition of “annual turnover” in clause 6D of the Bill.
Item 5. **Subsection 6(1) (definition of approved privacy code)**

14. Item 5 inserts a definition of “approved privacy code” in subsection 6(1) of the Act. The term “approved privacy code” is defined to mean a privacy code that has been approved by the Privacy Commissioner under clause 18BB, or a code that has been approved by the Privacy Commissioner under clause 18BB with variations approved by the Commissioner under clause 18BD. “Privacy code” is defined at Item 23 to mean a written code regulating acts and practices that affect privacy.

Item 6. **Subsection 6(1) (definition of breach an approved privacy code)**

15. Item 6 refers to the definition of “breach an approved privacy code” in clause 6B of the Bill.

Item 7. **Subsection 6(1) (definition of breach an Information Privacy Principle)**

16. Item 7 refers to the definition of “breach an Information Privacy Principle” in existing subsection 6(2) of the Act.

Item 8. **Subsection 6(1) (definition of breach a National Privacy Principle)**

17. Item 8 refers to the definition of “breach a National Privacy Principle” in clause 6A of the Bill.

Item 9. **Subsection 6(1) (definition of code complaint)**

18. Item 9 inserts a definition of “code complaint” in subsection 6(1) of the Act. The term “code complaint” is defined to mean a complaint about an act or practice that (if established) would be an interference with privacy because the act or practice breached an approved privacy code.

Item 10. **Subsection 6(1) (definition of Commonwealth contract)**

19. Item 10 inserts a definition of “Commonwealth contract” in subsection 6(1) of the Act. The definition covers any contract to which the Commonwealth or an agency is or was a party, under which services are or were provided to a Commonwealth
agency. The definition therefore includes contracts which have been completed or terminated. When read with Item 35, the definition also extends to the provision of services by the contracted service provider to other persons in connection with the performance of the Commonwealth agency’s functions. When read with the definition of “sub-contractor”, a Commonwealth contract extends to the provision of services by sub-contractors.

Item 11. Subsection 6(1) (definition of contracted service provider)

20. Item 11 inserts a definition of “contracted service provider” in subsection 6(1) of the Act. When read with the definitions of “government contract”, “Commonwealth contract” and “subcontractor”, the definition covers any person who, under a contract with the Commonwealth or an “agency” is or was responsible for the provision of services to a Commonwealth agency, either directly or as a subcontractor. When read with the definitions of “government contract”, “State contract” and “subcontractor”, the definition covers any person who, under a contract with a State or Territory or State or Territory authority, is or was responsible for the provision of services to a State or Territory authority, either directly or as a subcontractor.

21. The use of the past tense in this definition ensures that the provisions concerning contracted service providers continue even after the completion or termination of the contract. It also ensures that complaints about the acts and practices of contracted service providers under a Commonwealth contract may be taken to the Privacy Commissioner under Part V of the Act about breaches of a National Privacy Principle or an approved privacy code in relation to personal information held under or for the purposes of a Commonwealth contract even after the completion or termination of the contract.

Item 12. Subsection 6(1) (definition of employee record)

22. Item 12 inserts a definition of “employee record” in subsection 6(1) of the Act. The definition is used in relation to the exemption of acts and practices of organisations in respect of their employee records in sub-clause 7B(3). The term
“employee record” is defined to mean a record of personal information relating to the employment of an employee. Examples include health information about the employee and personal information about any or all of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee’s personal and emergency contact details;
- the employee’s performance or conduct;
- the employee’s hours of employment;
- the employee’s salary or wages;
- the employee’s membership of a professional or trade association;
- the employee’s trade union membership;
- the employee’s recreation, long service, sick, personal, maternity, paternity or other leave;
- the employee’s health information;
- the employee’s taxation, banking or superannuation affairs.

This list of examples of personal information about the employment of an employee is not intended to be exhaustive.

**Item 13. Subsection 6(1) (definition of enforcement body)**

23. Item 13 inserts a definition of “enforcement body” in subsection 6(1) of the Act. The definition includes all police services (paragraphs (a) and (h)) and other enforcement bodies such as the National Crime Authority, Australian Customs
Service, the Australian Securities and Investment Commission, the NSW Crime Commission, the Independent Commission Against Corruption, the NSW Police Integrity Commission and the Queensland Criminal Justice Commission. Other bodies created to conduct criminal investigations and enquiries (similar to the authorities and bodies named above) may be prescribed as an enforcement body at a later date (paragraph (m)).

24. Bodies other than police services are covered to the extent necessary for the performance of law enforcement functions. Agencies and State bodies are included to the extent they are responsible for administering, or performing a function under, a law that imposes a penalty or sanction (such as the Department of Immigration and Multicultural Affairs) or a prescribed law. Prescription of a law for the purposes of paragraphs (f) and (n) will provide clarification that a body is an enforcement body to the extent that it administers a particular law.

25. Paragraphs (g) and (o) include other agencies and State or Territory authorities in the definition only to the extent that they are responsible for administering laws relating to the protection of the public revenue (such as the Australian Taxation Office).

26. The definition of “enforcement body” is particularly relevant for the purposes of National Privacy Principle 2.1(h) and National Privacy Principle 6.1(j) and (k). Organisations may disclose personal information to an enforcement body, by virtue of National Privacy Principle 2.1(h). National Privacy Principle 6.1(j) and (k) provide that an individual may be denied access to his or her personal information where it would prejudice activities being carried out by an enforcement body or where an enforcement body has requested that there be no access because providing access would be likely to cause damage to the security of Australia.

Item 14. Subsection 6(1) (definition of generally available publication)

27. Item 14 amends the definition of “generally available publication” in subsection 6(1) of the Act. The amendment refers to publications “however published”. It is
intended that a reference to “generally available publications” includes documents published both through traditional methods, as well as by electronic means.

**Item 15. Subsection 6(1) (definition of government contract)**

28. Item 15 inserts a definition of “government contract” in subsection 6(1) of the Act. When read with the definition of “Commonwealth contract” the definition covers any contract with the Commonwealth or an agency under which services are or were provided to a Commonwealth agency. When read with the definition of “State contract” the definition covers any contract with a State or Territory or State or Territory authority or an agency under which services are or were provided to that State or Territory.

**Item 16. Subsection 6(1) (definition of health information)**

29. Item 16 inserts a definition of “health information” in subsection 6(1) of the Act. The definition identifies three types of information that are health information.

30. Paragraph (a) of the definition of health information covers “personal information” (currently defined in subsection 6(1) of the Act) that also has the characteristic of being information or an opinion about any of the following three subjects:

- the health or disability (at any time) of an individual. It is intended that this may include information or opinion about an individual’s previous or future physical, mental or psychological health.

- an individual’s expressed wishes about the future provision of health services. This is information of a type that may be found, for instance, in enduring powers of attorney.

- a “health service” provided, or to be provided, to an individual. This is intended to capture, for example, information that an individual has received a particular type of treatment. The definition of “health service” is set out at Item 17.
31. Whilst paragraph (a) of the definition covers information about an individual’s genetic make-up, the National Privacy Principles are not intended to specifically address the complex privacy issues that arise in respect of the handling of genetic information.

32. Paragraph (b) of the definition of health information covers other personal information (that is, information of a type not covered by paragraph (a)) collected to provide, or in providing, a health service. It is considered that the sensitive context in which such information is provided merits its protection as “health information”. This personal information may be about the recipient of the health service (for example, the recipient’s financial circumstances) or about another individual (for example, the contact details of the recipient’s next of kin).

33. Paragraph (c) of the definition covers other personal information (that is, information of a type not covered by paragraphs (a) or (b)) collected in connection with the donation or intended donation by the individual of his or her body parts, organs or body substances, including blood or bone marrow. Paragraph (c) is intended to capture personal information collected by, for example, pathology services.

34. The definition is not intended to cover information or an opinion about the professional practices of a health service provider whose identity is apparent, or can reasonably be ascertained, from the information or opinion. This type of information is, however, protected under the National Privacy Principles as “personal information”.

35. This definition is relevant to determining the type of personal information that is subject to the additional protection in the National Privacy Principles for “health information”. It also enables organisations to ascertain the type of personal information that is “sensitive information” (“health information” is defined as a category of “sensitive information”).

**Item 17. Subsection 6(1) (definition of health service)**

36. Item 17 inserts a definition of “health service” in subsection 6(1) of the Act. The
term “health service” is defined to mean either of two activities. Under paragraph (a), a health service is an activity performed in relation to an individual that is intended or claimed by the individual or the person performing it to have one of three purposes:

- to assess, record, maintain or improve the individual’s health;
- to diagnose the individual’s illness or disability; or
- to treat the individual’s illness or disability, whether actual or suspected.

37. Under paragraph (b), a health service is defined to mean the dispensing or prescription of a drug or medicinal preparation by a pharmacist. This is recognised as a sensitive context in which health information is handled. The activity of dispensing is expressly included within the definition because it may be difficult to claim that it is an activity that has one of the three purposes set out in paragraph (a).

38. It is intended that this definition cover disability, aged care or palliative care services and activities for which a Medicare rebate is unavailable (eg, cosmetic surgery) provided that such activities are intended or claimed to meet one of these purposes. The definition is also intended to cover the provision of a health product that is part of, or incidental to, the provision of a health service (for example, the administering of a vaccine). However, the definition is not intended to cover the provision of a health product that occurs independently from the provision of a health service. For example, the mere obtaining of non-prescription drugs or medicinal products from a pharmacist or supermarket is not intended to be considered a health service.

39. This definition is relevant to determining what types of personal information fall within the meaning of sub-paragraphs (a)(ii) and (iii) and paragraph (b) of the definition of “health information” in Item 16. This definition is also relevant to the operation of National Privacy Principle 10.2, National Privacy Principle 10.3 and National Privacy Principle 2.3. These sub-principles concern the collection and disclosure of health information in the context of a “health service”.

64
Item 18. Subsection 6(1) (definition of journalism)

40. Item 18 inserts a definition of “journalism” in subsection 6(1) of the Act. The term “journalism” is defined to mean the practice of collecting, preparing for dissemination or disseminating news, current affairs, documentaries and other information to the public. In addition, commentary or opinion on, or analysis of, this kind of material is included in the definition. The term ‘journalism’ is defined for the purposes of the exemption for acts and practices in the course of journalism that is contained in new sub-clause 7B(4).

Item 19. Subsection 6(1) (definition of media organisation)

41. Item 19 inserts a definition of “media organisation” in subsection 6(1) of the Act. The term “media organisation” is defined to mean an organisation whose activities consist of or include journalism, that is, the collection, preparation for dissemination or dissemination of news, current affairs, documentaries and other information to the public. In addition, commentary or opinion on, or analysis of, this kind of material is included in the definition. The definition does not require a media organisation to be solely engaged in journalism. For example, an organisation which is primarily engaged in promoting and protecting the environment may still be a media organisation for the purposes of the Bill if part of its activities consist of disseminating news and other information about the environment and related issues to the Australian public.

Item 20. Subsection 6(1) (definition of National Privacy Principle)

42. Item 20 inserts a definition of “National Privacy Principle” in subsection 6(1) of the Act. The term “National Privacy Principle” is defined to mean a principle contained in Schedule 3.

Item 21. Subsection 6(1) (definition of NPP complaint)

43. Item 21 inserts a definition of “NPP complaint” in subsection 6(1) of the Act. The term “NPP complaint” is defined to mean a complaint about an act or practice that
(if established) would be an interference with privacy because the act or practice breached a National Privacy Principle.

Item 22. Subsection 6(1) (definition of organisation)

44. Item 22 refers to the definition of “organisation” in clause 6C of the Bill.

Item 23. Subsection 6(1) (definition of privacy code)

45. Item 23 inserts a definition of “privacy code” in subsection 6(1) of the Act. The term “privacy code” is defined to mean a written code regulating acts and practices that affect privacy.

Item 24. Subsection 6(1) (at the end of paragraphs (a), (d), (e) and (f) of the definition of record)

46. Item 24 amends the existing definition of “record” by inserting “or” at the end of the paragraphs (a), (d), (e) and (f). This makes it clear that a record is any of the things listed in paragraphs (a) to (c), but not any one of the things listed in paragraphs (d) to (h).

Item 25. Subsection 6(1) (after paragraph (f) of the definition of record)

47. Item 25 amends the existing definition of “record” by inserting a new paragraph (fa) after existing paragraph (f) of the definition. The paragraph exempts from the definition of "record" any records that are in the custody of the Archives and in relation to which the Archives has entered into arrangements concerning access to those records, with a person other than a Commonwealth institution. The effect of this amendment is that the Information Privacy Principles do not apply to the Archives in respect of such records.

Item 26. Subsection 6(1) (definition of registered political party)

48. Item 26 inserts a definition of “registered political party” in subsection 6(1) of the Act. The term “registered political party” is defined to mean a political party registered under Part XI of the Commonwealth Electoral Act 1918. A “registered
political party” is not an organisation for the purposes of the Act (see definition of “organisation” in clause 6C).

**Item 27. Subsection 6(1) (definition of sensitive information)**

49. Item 27 inserts a definition of “sensitive information” in subsection 6(1) of the Act. The definition is based on that used in the *European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* and the Privacy Commissioner’s National Principles for the Fair Handling of Personal Information. “Sensitive information” is a subset of personal information and is defined to mean information or an opinion about an individual’s: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record; or health information.

50. This definition is applicable to the operation of a number of provisions. It is relevant in determining the type of personal information that is subject to additional protection under the National Privacy Principles that deal with “sensitive information”. That additional protection includes National Privacy Principle 10 (which limits the collection of “sensitive information”) and the exclusion of “sensitive information” from National Privacy Principle 2.1(c). Moreover, the definition operates to limit the types of personal information which, under clause 13B, can be collected or disclosed between related bodies corporate without being an interference with the privacy of an individual.

**Item 28. Subsection 6(1) (definition of small business)**

51. Item 28 refers to the definition of “small business” in clause 6D of the Bill.

**Item 29. Subsection 6(1) (definition of small business operator)**

52. Item 29 refers to the definition of “small business operator” in clause 6D of the Bill.
Item 30. Subsection 6(1) (definition of State contract)

53. Item 30 inserts a definition of “State contract” in subsection 6(1) of the Act. The definition covers any contract to which a State or Territory or State or Territory authority is or was a party, under which services are or were provided to a State or Territory authority. The definition therefore includes contracts which have been completed or terminated. When read with Item 35, the definition also extends to the provision of services by the contracted service provider to other persons in connection with the performance of the State or Territory authority’s functions. When read with the definition of “sub-contractor”, a State contract extends to the provision of services by sub-contractors.

Item 31. Subsection 6(1) (definition of State or Territory authority)

54. Item 31 refers to the definition of “State or Territory authority” in clause 6C of the Bill.

Item 32. Subsection 6(1) (definition of subcontractor)

55. Item 32 inserts a definition of “subcontractor” in subsection 6(1) of the Act. It covers a person who, under a subcontract, is or was responsible for the provision of services to a Commonwealth agency, a State or Territory authority, or a contracted service provider. The definition is necessary to allow for the coverage of subcontractors as contracted service providers. As the definition of “contracted service provider” includes a “subcontractor”, the effect of this definition is to apply coverage to all subsequent subcontractors responsible for the provision of services for the purposes of a government contract.
Item 33. Subsection 6(1) (definition of temporary public interest determination)

56. Item 33 inserts a definition of “temporary public interest determination” in subsection 6(1) of the Act. The term “temporary public interest determination” is defined to mean a determination made under clause 80A of the Bill.

Item 34. At the end of subsection 6(7)

57. Item 34 inserts new paragraphs 6(7)(c), (d), (e) and (f). Currently subsection 6(7) provides that complaints may be both a file number complaint and an IPP complaint or a credit reporting complaint.

58. Paragraph 6(7)(c) provides that a complaint may be both a file number complaint and a code complaint. Paragraph 6(7)(d) provides that a complaint may be both a file number complaint and an NPP complaint. Paragraph 6(7)(e) provides that a complaint may be both a code complaint and a credit reporting complaint. Paragraph 6(7)(f) provides that a complaint may be both an NPP complaint and a credit reporting complaint.

59. Organisations that handle credit information and tax file numbers are still required to comply with the National Privacy Principles (or approved privacy code). It is possible, therefore, that there may be more than one adverse finding against an organisation, where an investigator finds that more than one set of standards has been breached. A complaint about a bank mishandling credit information may, for example, also involve an investigation into whether the bank complied with its obligations under the National Privacy Principles (or, where the bank has a privacy code approved by the Privacy Commissioner, whether the bank complied with its obligations under that code).

Item 35. Subsection 6(8)

60. Item 35 repeals current subsection 6(8) and inserts two new sub-clauses 6(8) and (9). Currently subsection 6(8) determines the question of whether one corporation is related to another corporation in the same way as the question is determined under the
Companies Act 1981. The new sub-clause 6(8) states that the question of whether one body corporate is related to another body corporate is to be determined in the same way as the question is determined under the Corporations Law. The definition is relevant to the credit reporting provisions (specifically sections 18N and 18Q) and in the interpretation of clause 13B, which exempts certain acts and practices from being interferences with privacy when information is collected from and disclosed by related bodies corporate.

61. Sub-clause 6(9) defines what services *provided* to an agency or State or Territory authority means. New sub-clause 6(9) ensures that “services provided to an agency or a State or Territory authority” (relevant to the definitions of “Commonwealth contract”, “contracted service provider”, “state contract” and “subcontractor”) include the provision of services to third parties on behalf of an agency or a State or Territory authority.

Item 36. After section 6

62. Item 36 inserts new clauses 6A, 6B, 6C, 6D, 6E and 6F. New clause 6A covers what it means to breach a National Privacy Principle. Sub-clause 6A(1) provides that a “breach of a National Privacy Principle” means an act or practice contrary to or inconsistent with that National Privacy Principle. Sub-clauses 6A(2), (3) and (4) list the circumstances in which an act or practice will not be a breach of a National Privacy Principle. Sub-clause 6A(5) provides that these sub-clauses have effect despite sub-clause 6A(1).

63. Sub-clause 6A(2) relates to contracted service providers. The sub-clause provides that an act or practice will not breach a National Privacy Principle if it is done, or engaged in, by an organisation that is a contracted service provider for a Commonwealth contract, it is for the purpose of meeting obligations under that contract and it is authorised by a provision of the contract that is inconsistent with the National Privacy Principle. The effect of this provision is that a privacy clause in a Commonwealth contract that is inconsistent with a National Privacy Principle will prevail over that National Privacy Principle. If a clause in a Commonwealth contract
is consistent with a National Privacy Principle or there is no corresponding clause in the Commonwealth contract, a National Privacy Principle will apply to the contracted service provider and the general rule regarding breach of a National Privacy Principle will apply.

64. Sub-clause 6A(3) relates to the provision of information to the Archives. It confirms that disclosing personal information contained in a record to the Archives is allowed (that is, it will not be a breach of the National Privacy Principles), where the disclosure is solely for the purpose of enabling the Archives to consider whether or not to accept custody of the record.

65. Sub-clause 6A(4) provides that an act or practice which occurs outside Australia does not breach a National Privacy Principle if the act or practice is required by an applicable law of a foreign jurisdiction. This provision is intended to ensure that the extra-territorial operation of the Act does not require organisations to act in contravention of laws operating in the country in which the act or practice occurs.

66. New clause 6B covers what it means to breach an approved privacy code. Sub-clause 6B(1) provides that a “breach of an approved privacy code” means an act or practice contrary to or inconsistent with that approved privacy code. An approved privacy code is defined in subsection 6(1) to mean a privacy code that has been approved by the Privacy Commissioner after consideration of the matters in clause 18BB.

67. Sub-clauses 6B(2), (3) and (4) list the circumstances in which an act or practice will not be a breach of an approved privacy code. Sub-clause 6A(5) provides that these sub-clauses have effect despite sub-clause 6A(1).

68. Sub-clause 6B(2) relates to organisations that are contracted service providers. The sub-clause provides that an act or practice will not breach an approved privacy code if it is done, or engaged in, by an organisation that is a contracted service provider for a Commonwealth contract, it is for the purpose of meeting obligations under that contract and it is authorised by a provision of the contract that is
inconsistent with that approved privacy code. The effect of this provision is that a privacy clause in a Commonwealth contract that is inconsistent with an approved privacy code will prevail over that code. If a clause in a Commonwealth contract is consistent with the code or there is no corresponding clause in the Commonwealth contract, an approved privacy code will apply to the contracted service provider and the general rule regarding breach of a code will apply.

69. Sub-clause 6B(3) relates to the provision of information to the Archives. It confirms that disclosing personal information contained in a record to the Archives is allowed (that is, it will not be a breach of an approved privacy code), where the disclosure is solely for the purpose of enabling the Archives to consider whether or not to accept custody of the record.

70. Sub-clause 6B(4) provides that an act or practice which occurs outside Australia does not breach an approved privacy code if the act or practice is required by an applicable law of a foreign jurisdiction. This provision is intended to ensure that the extra-territorial operation of the Act does not require organisations to act in contravention of laws operating in the country in which the act or practice occurs.

71. New clause 6C inserts a definition of “organisation”. The term “organisation” defines the range of private sector bodies and persons to whose acts and practices the Bill applies. An “organisation” must not do acts or engage in practices that breach an approved privacy code or, to the extent that an organisation is not bound by an approved privacy code, the National Privacy Principles.

72. “Organisation” is defined in sub-clause 6C(1) to mean an individual, a body corporate, a partnership, any other unincorporated association, or a trust, but does not include a small business operator (as defined in clause 6D); an agency (an agency is already required to comply with the Information Privacy Principles); a registered political party (as defined in subsection 6(1)); a State or Territory authority (as defined in sub-clause 6C(3)); or a State or Territory instrumentality that has been prescribed as such by regulation in accordance with the requirements in sub-clause 6C(4). In this clause a reference to State does not include the Australian Capital Territory or the
Northern Territory (sub-clause 6C(5)). Sub-clause 6C(2) confirms that a legal person may have a number of different capacities in which the person does things.

73. Sub-clause 6C(3) defines a “State or Territory authority”. State or Territory authorities are, in general terms, defined to mean people or bodies that are part of the State or Territory public sector (e.g.: Ministers, Departments and Courts. Local Government Councils will generally fall within the definition at paragraph 6C(3)(c)). It is not intended to regulate the acts and practices of a State or Territory public sector. This is left for the States and Territories to regulate. State or Territory statutory corporations are excluded from the coverage of the Bill by virtue of paragraph 6C(3)(c), but Government Business Enterprises that are Corporation Law corporations will be covered unless they are prescribed in accordance with sub-clause 6C(4).

74. Sub-clause 6C(4) describes the process for making regulations that stop State or Territory instrumentalities from being organisations (if a State or Territory instrumentality is not an organisation, its acts and practices are not regulated by the Bill). One of the purposes of this sub-clause is to recognise that Commonwealth regulation of a State or Territory instrumentality (for example a Corporations Law company, society or association) that performs core government functions is inappropriate, if such regulation would curtail the capacity of the State or Territory to function as a government. Before the Governor-General may make regulations prescribing a State or Territory instrumentality, the Minister must be satisfied that the State or Territory has requested that the instrumentality be prescribed as such and must then consider several matters listed in subparagraphs 6C(4)(b)(i), (ii) and (iii). The Minister is, under paragraph 6C(4)(b), required to consider whether the government of a State or Territory would be adversely affected if a particular instrumentality was regulated by the Bill and, in consultation with the Privacy Commissioner, the desirability of regulating the handling of personal information by the instrumentality through the Bill and whether a law of a State or Territory would regulate the handling of personal information by the instrumentality to a standard at least equivalent to the standard in the Bill.
75. Clauses 6D and 6E describe how the Bill applies to small businesses. By virtue of the definition of “organisation” at Clause 6C, “small business operators” are not organisations and are consequently exempt from the operation of the Bill. Clause 6D describes what a small business is and when a small business is a “small business operator”. Some small businesses (those small businesses that engage in acts or practices that pose a particular risk to the privacy of individuals) will not be small business operators and will therefore remain subject to the provisions of the Bill.

76. Sub-clause 6D(1) defines a small business as a business with an annual turnover of $3 million or less. Subclause 6D(2) defines “annual turnover”. Annual turnover is calculated in the same manner as in the *A New Tax System (Goods and Services) Act 1999*.

77. If an organisation has carried on a business for the 11 months preceding the month in which the annual turnover is calculated and did not carry on another business in the preceding 12 months, the “annual turnover” for that business is defined to mean the organisation’s current annual turnover as worked out in accordance with subsection 188-15(1) of the *A New Tax System (Goods and Services Tax) Act 1999*.

78. If an organisation has carried on a business for the 11 months preceding the month in which the annual turnover is calculated and also carried on another business in the preceding 12 months, the organisation’s “annual turnover” is defined to be its current annual turnover worked out in accordance with subsection 188-15(1) of the *A New Tax System (Goods and Service Tax) Act 1999* disregarding supplies made or likely to be made by the organisation otherwise than in the course of the first-mentioned business.

79. If an organisation has not carried on a business for the 11 months preceding the month in which the annual turnover is calculated, the organisation’s “annual turnover” is defined as its projected annual turnover worked out in accordance with subsection 188-20(1) of the *A New Tax System (Goods and Services Tax) Act 1999* disregarding supplies made or likely to be made otherwise than in the course of the business.
The term “supplies” is defined in the *A New Tax System (Goods and Services Tax) Act 1999*. The use of the GST methodology was adopted so as to minimise compliance costs on businesses by allowing them to use their taxation calculations for the purposes of the Act.

Sub-clause 6D(3) provides that a small business operator is an individual, body corporate, partnership, unincorporated association or trust that carries on one or more small businesses but does not carry on a business that is not a small business. This definition is designed to ensure that a large enterprise that, among other things, carries on a business that would fall within the definition of small business, cannot benefit from being characterised as a small business operator.

Sub-clause 6D(4) specifies those small businesses that are not small business operators for the purposes of the Bill. Small businesses that fall within paragraphs 6D(4)(a), (b), (c), (d) or (e) are organisations for the purposes of the Bill and are therefore subject to its provisions. Paragraph 6D(4)(a) provides that an individual, body corporate, partnership, unincorporated association or trust is not a small business operator if, at any time after the business was started or the commencement of this section, the business has an annual turnover of more than $3 million. Paragraph 6D(4)(b) provides that a small business that provides a health service and holds health information, except in an employee record, is not a small business operator. Paragraph 6D(4)(c) provides that a small business that discloses personal information about another individual to anyone else for service, benefit or advantage is not a small business operator. Conversely, paragraph 6D(4)(d) provides that a small business that provides a benefit, service or advantage to collect personal information about another individual from anyone else is not a small business operator. And finally, paragraph 6D(4)(e) provides that a contracted service provider for a Commonwealth contract is not a small business operator.

Sub-clause 6D(5) confirms that an individual will not be prevented from being a small business operator merely if he or she does something described in paragraphs 6D(4)(b), (c) or (d) otherwise than in the course or carrying on his or her business and
only for the purposes of or in connection with his or her personal, family or household affairs.

84. Sub-clause 6D(6) confirms that a body corporate, partnership, unincorporated association or trust will not be prevented from being a small business operator because it does something described in paragraphs 6D(4)(b), (c) or (d) otherwise than in the course or carrying on its business.

85. Clause 6E allows regulations to be made prescribing small business operators and particular acts and practices of small business operators. Once prescribed, the Bill will apply (with the prescribed modifications if any) to the small business operator, either in relation to all of the small business operator’s acts and practices or the particular acts and practices that were prescribed, as if the small business operator were an organisation. The regulations may also prescribe small business operators, or acts and practices of small business operators, by reference to a particular class of small business operator (for example, “used car dealers”), or class of act or practice of small business operators (for example, the act of collecting information about the religion of customers). Under sub-clause 6E(3), modifications include additions, omissions and substitutions.

86. Sub-clause 6E(4) provides that before the Governor-General may make regulations under clause 6E, the Minister must be satisfied that it is in the public interest to regulate the small business operator (or act or practice) in question, and must consult the Privacy Commissioner about the desirability of regulating the small business operator, act or practice.

87. Clause 6F allows a State or Territory instrumentality that has been prescribed (and is therefore no longer an organisation for the purpose of the Bill) to opt back in to coverage by the Bill in a modified way. In such a case, the Bill would apply to regulate the handling of personal information (with the prescribed modifications) as if the instrumentality were an organisation. Clause 6F also describes how a State or Territory authority not otherwise covered by the Bill, (because it is not, by definition, an organisation) may choose to “opt in” to the privacy regime in the Bill, by
The State or Territory may request that the Act apply to the authority in a modified way. Under sub-clause 6F(2), modifications include additions, omissions and substitutions. Before the Governor General is able to make regulations prescribing a State or Territory authority, the Minister must be satisfied that the relevant State or Territory has requested that the authority be prescribed, and consult with the Privacy Commissioner about the desirability of regulating the acts and practices of the authority under the Bill (sub-clause 6F(3)). Once prescribed, the Bill applies (with the prescribed modifications, if any) to the prescribed authority as if it were an organisation (sub-clause 6F(1)). One of the purposes of this clause is to allow statutory corporations whose activities are predominantly commercial, to opt in to the private sector privacy regime where the State (or Territory) and Minister (in consultation with the Privacy Commissioner) consider that it is appropriate to do so.

Item 37. Application

88. Item 37 confirms that a Commonwealth contract may prevent an act or practice from being a breach of a National Privacy Principle or an approved code regardless of when the contract was made (ie: before or after the commencement of clauses 6A and 6B).

Item 38. At the end of paragraph 7(1)(ed)

89. Item 38 inserts “or” after paragraph 7(1)(ed) in order to allow for an additional provision in relation to the acts and practices of organisations to be included in the list of acts and practices to which the Act applies. The heading to section 7 is consequentially amended by inserting “organisations” after “agencies”.

Item 39. After paragraph 7(1)(ed)

90. Item 39 inserts a new paragraph 7(1)(ee). Currently subsection 7(1) defines what is meant by a reference to an act or practice in the Act. New paragraph 7(1)(ee) adds an act done, or practice engaged in, by an organisation (other than an exempt act or practice), to the list of acts or practices to which the Act applies.
Item 40. Subsection 7(2)

91. Item 40 amends subsection 7(2). The Act does not currently apply the Information Privacy Principles to acts and practices of the bodies listed in Part 1 of Schedule 2 and Division 1 of Part II of Schedule 2 to the Freedom of Information Act 1982 (the FOI Act). The amendment to subsection 7(2) inserts “National Privacy Principles, an approved privacy code” so that the Act will not apply the Information Privacy Principles, National Privacy Principles or an approved code to acts and practices of the bodies listed in Part 1 of Schedule 2 or Division 1 of Part II of Schedule 2 of the FOI Act. An agency listed in Part 1 of Schedule 2 may be prescribed for the purpose of clause 7B. In that case, the acts and practices of the prescribed agency are treated as being acts and practices of an organisation (and the prescribed agency is treated as an organisation). Where an agency has been prescribed, the National Privacy Principles (or approved privacy code, where appropriate) will apply to the prescribed agency.

Item 41. Subsection 7(4)

92. Item 41 amends subsection 7(4). Subsection 7(4) refers to paragraphs in section 27, and these references are consequentially amended to reflect the changes that have been made to the paragraphs in section 27.

Item 42. After section 7

93. Item 42 inserts new clauses 7A, 7B and 7C. The effect of new clause 7A is to make the acts and practices of some agencies subject to the standards in the National Privacy Principles (or an approved privacy code, as appropriate), to the extent that they are not currently subject to the Information Privacy Principles (by virtue of section 7 of the Act). The Government’s policy is that bodies operating in the commercial sphere should operate on a level playing field. Where agencies are engaged in commercial activities, they should be required to comply with the National Privacy Principles, just like private sector organisations. The purpose of this clause which, (by virtue of sub-clause 7A(4)) has effect despite existing subparagraph
7(1)(a)(i), paragraph 7(1)(c) and subsection 7(2), is to give effect to this policy.

94. New clause 7A affects agencies specified in Part I of Schedule 2 of the FOI Act that have been prescribed for the purpose of sub-clause 7A(2). Sub-clause 7A(1) provides that acts and practices of prescribed agencies will be subject to the Act as if the agency were an organisation. Agencies that are in Part I of Schedule 2 of the FOI Act do not currently have to comply with the Information Privacy Principles. The aim of the amendment is to make some of those agencies (to be prescribed by regulation at a later date) comply with the Act. The result is that these agencies will need to comply with the National Privacy Principles (or an approved privacy code, as appropriate).

Sub-clause 7A(1) foreshadows that it may be appropriate for the Act to be modified in its application to prescribed agencies. “Modifications” is defined in sub-clause 7A(5).

95. Clause 7A also affects the acts and practices of agencies in Division 1 of Part II of Schedule 2 to the FOI Act (to the extent that the acts and practices relate to documents associated with the agency’s commercial activities or the commercial activities of another entity) (sub-clause 7A(3)). Sub-clause 7A(1) provides that acts and practices described in sub-clause 7A(3) will be subject to the Act as if the act or practice were an act done or a practice engaged in by an organisation and the agency mentioned in that sub-clause were an organisation. Agencies in Division 1 of Part II of Schedule 2 to the FOI Act are not currently required to comply with the Information Privacy Principles (in relation to documents in respect of the agency’s commercial activities or the commercial activities of another entity). The aim of the amendment is to ensure that an agency in Division 1 of Part II of Schedule 2 to the FOI Act complies with the standards set out in the National Privacy Principles or an approved privacy code (as appropriate) in relation to documents in respect of its commercial activities or the commercial activities of another entity. This clause is intended to apply to agencies such as Comcare, the Health Insurance Commission and Telstra Corporation Limited. It is not intended to apply to the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.

96. New clause 7B sets out acts and practices of organisations that are exempt for the
purposes of new paragraph 7(1)(ee). The effect of this provision is to exempt certain
acts and practices from the operation of the Bill.

97. Sub-clause 7B(1) exempts acts done or practices engaged in by individuals
where those acts are done, or practices are engaged in, other than in the course of
business. The Act is not intended to affect the way an individual collects, holds, uses,
discloses, or transfers personal information in the course of his or her personal, family
or household affairs.

98. Sub-clause 7B(2) deals with the situation where a small business is also a
contracted service provider for a Commonwealth contract. It provides that an act done
or practice engaged in by such an organisation, is exempt for the purposes of
paragraph 7(1)(ee) provided the act is done or practice engaged in otherwise than for
the purpose of meeting an obligation under a Commonwealth contract. An
organisation to which this sub-clause applies, therefore, need only comply with the
legislation in relation to its activities that are for the purposes of a Commonwealth
contract. In relation to its activities that are not for the purposes of a Commonwealth
contract, the organisation is in the same position as a small business operator.

99. This sub-clause applies to a contracted service provider that is a party to the
Commonwealth contract and to a subcontractor who may not be a party to that
contract but is a party to a subcontract where the act done, or practice engaged in, is
directly or indirectly for the purposes of meeting an obligation under the contract.

100. Sub-clause 7B(3) exempts acts done or practices engaged in by an organisation
that is or was an employer of an individual where the act or practice is directly related
to a current or former employment relationship between the employer and the
individual and an “employee record” relating to the individual. The act or practice
must be directly related to a current or former employment relationship so as to ensure
that employers cannot use “employee records” for commercial purposes unrelated to
the employment context. Acts and practices in relation to “employee records” are
exempted as it is recognised that the handling of employee records is a matter better
dealt with under workplace relations legislation.
101. Sub-clause 7B(4) exempts acts and practices engaged in by an organisation where the act is done or practice is engaged in, “in the course of journalism”. This exemption seeks to balance the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media. This aim is also made clear in clause 3, which sets out the objects of the Act.

102. Sub-clause 7B(5) exempts acts and practices of an organisation acting under a State contract where the act done, or practice engaged in, is directly or indirectly, for the purposes of meeting an obligation under that contract. This ensures that private sector organisations providing services under contract to a State or Territory authority are exempt from the Commonwealth’s privacy regime in respect of those services and can be regulated by the relevant State or Territory.

103. Clause 7C exempts political acts and practices from the operation of the Act.

104. Sub-clause 7C(1) exempts acts done, or practices engaged in, by an organisation that is either a member of Parliament or a councillor of a local government authority, where the acts are done, or practices are engaged in, for a purpose that is connected to an election under an electoral law, a referendum under a law of the Commonwealth or State or Territory, or the participation of the member or councillor in any aspect of the political process.

105. Sub-clause 7C(2) exempts acts done or practices engaged in, by an organisation that is a contractor, for the purposes of paragraph 7(1)(ee), if the act is done or practice is engaged in for the purpose of meeting an obligation under a contract between the contractor and a registered political party, or a member of Parliament or councillor described in sub-clause 7C(1), and for any purpose outlined in paragraph 7C(2)(b).

106. Sub-clause 7C(3) exempts acts done, or practices engaged in, by an organisation that is a sub-contractor to a contractor described in sub-clause 7C(2), where the act is done or practice is engaged in for the purposes of meeting an obligation under a contract between the contractor and the sub-contractor and for a purpose referred to in
107. Sub-clause 7C(4) exempts acts done or practices engaged in voluntarily by an organisation for or on behalf of a registered political party for a purpose listed in paragraphs 7C(4)(a) to (c) or facilitating acts or practices of a registered political party for a purpose mentioned in paragraphs (a) to (c).

108. Sub-clause 7C(5) clarifies that sub-clause 7C(4) does not otherwise affect the operation of the Act in relation to agents or principals.

109. Sub-clause 7C(6) defines the meaning of “electoral law” and “Parliament”. “Electoral law” is defined to mean a law of the Commonwealth, or State or Territory, relating to elections to Parliament or a local government authority. “Parliament” is defined to mean the Parliament of the Commonwealth or a State, or the legislature of a Territory.

**Items 43 and 44. Paragraph 8(1)(a)**

110. Item 43 inserts “organisation” into paragraph 8(1)(a) after “an agency” and Item 44 inserts “organisation” into the paragraph after “the agency”. The heading to section 8 is consequentially amended to read “Acts and practices of, and disclosure of information to, staff of agency, organisation etc”. Currently, paragraph 8(1)(a) states that an act done or practice engaged in by, or information disclosed to, a person in the course of employment by or in the service of an agency, file number recipient, credit reporting agency or credit provider, shall be treated as having been done, engaged in by or disclosed to the agency. Items 43 and 44 insert “organisation” into the paragraph so that acts done or practices engaged in by, or information disclosed to, a person in the course of employment by, or in the service of, an organisation will also be treated as having been done, engaged in by, or disclosed to, the organisation. An individual employed by an organisation is not considered to be an “organisation” himself or herself.

**Item 45. Paragraph 8(1)(b)**
111. Item 45 inserts “or organisation” into paragraph 8(1)(b) after “an agency”.

**Item 46. Paragraph 8(1)(b)**

112. Item 46 inserts “or organisation” into the paragraph after “the agency”. This item, together with Item 45, extends the application of existing paragraph 8(1)(b) and deems an act done or practice engaged in by, or information disclosed to, a person on behalf of, or for the purposes of the activities of an unincorporated body (as currently defined in paragraph 8(1)(b)), for the purpose of assisting, or performing functions in connection with an organisation is to be deemed as having been done, or engaged in by, or disclosed to, that organisation.

**Item 47. At the end of section 8**

113. Item 47 inserts new sub-clauses 8(3), (4) and (5) at the end of section 8. These sub-clauses relate to partnerships, unincorporated associations and trusts. They describe how the Act applies to these non legal entities, specifically identifying whose acts and practices constitute acts and practices of the organisation, and to whom a communication must be made in order to communicate with the organisation.

114. Sub-clause 8(3) provides, in relation to partnerships, that an act or practice of a partner is taken to be an act or practice of the organisation, and that a communication made to a partner is taken to have been made to the organisation.

115. Sub-clause 8(4) provides, in relation to unincorporated associations, that an act or practice of a member of the committee of management of the association is taken to be an act or practice of the organisation, and that a communication made to a member of the committee of management of the association is taken to have been made to the organisation.

116. Sub-clause 8(5) provides, in relation to trusts, that an act or practice of a trustee is taken to be an act or practice of the organisation, and that a communication made to a trustee is taken to have been made to the organisation.

**Item 48. At the end of Part II**
117. Item 48 inserts a new clause 12B. Clause 12B is intended to ensure that the Act is given the widest possible operation consistent with Commonwealth constitutional legislative power. Sub-clause 12B(1) provides that, without limiting the effect of the Act apart from section 12B, the Act also has effect as provided by each of sub-clauses 12B(2) to (8), namely, the Act has the effect it would have if its operation in relation to organisations were expressly confined to:

- giving effect to the International Covenant on Civil and Political Rights, and in particular, Article 17 of the Covenant;

- acts or practices by organisations covered by sub-clause 5B(1) which occur outside Australia and the external Territories;

- organisations which are corporations;

- acts or practices of organisations taking place in the course of, or in relation to, trade or commerce between Australia and places outside Australia, among the States or within a Territory, between a State and a Territory or between two Territories;

- acts or practices of organisations taking place using a postal, telegraphic, telephonic or other like service within the meaning of paragraph 51(v) of the Constitution;

- acts or practices of organisations taking place in a Territory;

- acts and practices of organisations taking place in a place acquired by the Commonwealth for public purposes.

**Item 49. Before section 13**

118. Item 49 inserts the heading “Division 1 - Interferences with privacy” before section 13 of the Act.
119. Section 13 marks the beginning of Part III of the Act. The amendments in this Bill separate Part III of the Act into five divisions. Division 1 relates to interferences with privacy generally. Division 2 relates to duties and obligations of public sector bodies and contains the Information Privacy Principles. Division 3 relates to duties and obligations of private sector bodies. Division 4 relates to duties and obligations of tax file number recipients. Division 5 relates to duties and obligations in respect of credit information files and credit reports.

**Item 50. Section 13**

120. Item 50 amends section 13 by deleting the words “and only if”. The amendment recognises that an act or practice may also be an interference with the privacy of an individual under clause 13A.
Item 51. Paragraphs 13(b) and (d)

121. Item 51 amends paragraphs 13(b) and 13(d) by inserting “organisation” after “an agency”. The affect of this amendment is to extend the application of the provisions to organisations.

122. The amendment recognises that a file number recipient may also be an organisation and confirms that an act or practice engaged in by a file number recipient that is an organisation is an interference with privacy if it breaches a guideline under section 17 (in relation to tax file numbers). A credit reporting agency or credit provider may also be an organisation and the amendment further recognises that an act or practice engaged in by a credit reporting agency or credit provider that is an organisation is an interference with privacy if it constitutes a credit reporting infringement.

Item 52. After section 13

123. Item 52 inserts new clauses 13A to F.

124. Clause 13A establishes the elements of an interference with the privacy of an individual by an organisation. Sub-clause 13A(1) lists what constitutes an “interference with privacy” by an organisation. The general rule is that an act or practice of an organisation is an interference with privacy if:

(a) the act or practice breaches an approved privacy code that binds the organisation, or

(b) where the organisation is not bound by an approved privacy code, the act or practice breaches a National Privacy Principle, or

(c) the act or practice relates to personal information that relates to the individual; the organisation is a contracted service provider for a Commonwealth contract; the Commonwealth contract includes a provision that is inconsistent with an approved code or the National Privacy Principles; and the act done, or
practice engaged in, is inconsistent with the relevant provision of the contract; or

(d) where the organisation is a contracted service provider under a Commonwealth contract, the organisation uses or discloses the personal information obtained for the purpose of meeting an obligation under a Commonwealth contract for direct marketing (in contravention of clause 16F).

125. Sub-clause 13A(2) recognises that the general rule applies even if other rules apply by virtue of the organisation being a credit reporting agency, credit provider or a file number recipient. Note that clause 13E confirms that the exceptions in clauses 13B, 13C and 13D do not over ride other obligations that an organisation may have by virtue of being a credit reporting agency, credit provider, or file number recipient.

126. Clause 13B identifies situations where acts and practices of related bodies corporate will not be interferences with privacy. Sub-clause 13B(1) recognises commercial reality that, for many bodies corporate to continue to operate effectively, they need to be able to communicate with related bodies corporate. Often, what appears to the consumer to be one “organisation” will in fact (by virtue of the definition of “organisation” in clause 6C) be several bodies corporate that are related to each other. The effect of clause 13B is to allow one body corporate to disclose information to another body corporate that is related to it, without the disclosure being an interference with privacy. The clause also allows the collection by the related body corporate from the first body corporate. The bodies corporate will, in all other areas, each need to comply with the National Privacy Principles (or approved privacy code, as appropriate).

127. Before an organisation can collect personal information and rely on sub-clause 13B(1) to allow it to disclose to other bodies corporate to which it is related, it must first comply with National Privacy Principle 1.3 or 1.5 (or code equivalent, whichever is appropriate). National Privacy Principle 1.3 (which applies where personal information is collected directly from the individual) and National Privacy Principle 1.5 (which applies where information is collected from a third party) both require the organisation to take reasonable steps to ensure that the individual knows that the
organisation has collected the information, what the organisation will use the information for, and the types of organisations to which the information is usually disclosed by that organisation. These sub-principles aim to ensure that individuals are aware of who has their personal information and what the information will be used for. An approved privacy code will also contain equivalent (or greater) privacy protection.

128. The exemption is limited to the collection from, and disclosure by, related bodies corporate of personal information that is not “sensitive information”. Sub-clause 13B(1) does not allow the disclosure of health information between private hospitals or between co-located private hospitals and community held centres run by related bodies corporate.

129. The note for sub-clause 13B(1) confirms that the provision allows related bodies corporate to share personal information but that handling of the personal information is still subject to the National Privacy Principles (or approved privacy code, as appropriate). The National Privacy Principles contain a new sub-principle (2.3) that clarifies how an organisation may use personal information collected from a related body corporate. The new sub-principle defines the meaning of “primary purpose” in terms of the main purpose for which the personal information was originally collected. This means that the “primary purpose” is transferred with the personal information when it is shared around the group of related bodies corporate. Each body corporate within the group must use the information consistently with the main purpose for which it was originally collected, and may only use the personal information for a secondary purpose where that purpose is allowed by National Privacy Principle 2.1 (or equivalent provision in an approved privacy code).

130. Sub-clause 13B(2) confirms that 13B(1) does not over-ride the general rule for organisations that are contracted service providers.

131. Clause 13C identifies situations where acts and practices of partnerships will not be interferences with privacy. The sub-clause is intended to address what happens to personal information that is in the possession of a partnership when that partnership dissolves, and a new partnership (with at least one partner in common with the first
partnership) forms to carry on the same, or a similar, business. For example, a law firm (a partnership) collects personal information from, and holds personal information about, its clients. If a partner leaves the partnership, and a new partner joins the firm, the first partnership has dissolved and a second partnership forms. The purpose of clause 13C is to prevent disclosure to the second partnership and collection by the second partnership from being an interference with privacy. The sub-clause is not intended to allow a partnership to reform and use the information collected for a totally different business purpose.

132. The note for sub-clause 13C(1) confirms that personal information may be passed from an old partnership to a new partnership but that handling of the personal information is still subject to the National Privacy Principles (or approved privacy code, as appropriate).

133. Clause 13D provides that an act or practice which occurs outside Australia is not an interference with privacy if the act or practice is required by an applicable law of a foreign jurisdiction. This provision is intended to ensure that the extra-territorial operation of the Act does not require organisations to act in contravention of laws operating in the country in which the act or practice occurs.

134. Clause 13E confirms that the exceptions in clauses 13B, 13C and 13D are subject to section 13 of the Act (which identifies acts and practices that are interferences with privacy). For example, a credit provider can not rely on clause 13B to pass credit information to a related body corporate. Disclosure of credit information can be made to a related corporation under paragraph 18N(1)(d), but the related corporation must not use or disclose the information except in accordance with section 18Q of the Act.

135. Clause 13F recognises that section 13 of the Act and clause 13A provide an exhaustive description of what constitutes an interference with privacy.

136. The heading “Division 2 - Information Privacy Principles” is inserted.

Item 53. Application
137. Item 53 confirms that an act or practice of an organisation that is a contracted service provider for a Commonwealth contract may be an interference with privacy under paragraph 13A(1)(c) whether the contract was made before or after the commencement of clause 13A.

**Item 54. After section 16**

138. Item 54 inserts a new Division 3 headed “Approved privacy codes and the National Privacy Principles”, which comprises clauses 16A, 16B, 16C, 16D, 16E and 16F.

139. Clause 16A requires organisations to comply with an approved privacy code, or, to the extent that an organisation is not bound by an approved privacy code, to refrain from doing an act, or engaging in a practice, that breaches the National Privacy Principles.

140. Sub-clause 16A(3) clarifies that clause 16A, approved privacy codes and the National Privacy Principles have effect in addition to the existing requirements placed on the Privacy Commissioner to issue a Code of Conduct relating to credit information files and credit reports, and the existing provisions in relation to credit reporting generally.

141. Sub-clause 16A(4) confirms that an act or practice is not authorised by law for the purposes of existing Part IIIA (credit reporting), merely because it does not breach an approved privacy code or the National Privacy Principles.

142. The criteria and procedure for approval of privacy codes are dealt with in Part IIIAA. Before a privacy code may be approved by the Privacy Commissioner the code must provide as least as much privacy protection as the National Privacy Principles. The National Privacy Principles are contained in Schedule 3 to the Act, and provide default minimum standards for the handling of personal information.

143. Clause 16B specifies when the Act applies to personal information collected and held by an organisation. The Act applies to personal information being collected by an
organisation if the organisation collects it for inclusion in a “record” or “generally available publication” (as defined in section 6). The Act applies to personal information that has been collected by an organisation if the organisation holds the information in a record.

144. Clause 16C comprises sub-clauses 16C(1), (2), (3) and (4). Sub-clause 16C(1) restricts the application of National Privacy Principles 1 and 3 (in so far as these relate to the collection of personal information) and 10 to collection of information that occurs after commencement of the clause. Sub-clause 16C(2) provides that National Privacy Principles 3 (in so far as it relates to the use or disclosure of personal information), 4, 5, 7 and 9 apply to personal information held by an organisation, whether that information was collected before or after commencement of this clause. Sub-clause 16C(3) restricts the application of National Privacy Principles 2 and 6 to personal information collected after commencement of this clause. Sub-clause 16C(4) restricts the application of National Privacy Principle 8 to transactions entered into after the commencement of this clause.

145. Clause 16D delays the application of the National Privacy Principles to organisations that carry on one or more small businesses (but do not carry on any other business) for a period of 12 months, starting when clause 16D commences. Clause 16D will commence at the same time as the rest of the Bill. The delayed commencement is designed to allow small businesses extra time to ensure compliance with the legislation. After the initial period, it is intended that small businesses be exempt from the operation of the legislation where the nature of their business means that they constitute a low privacy risk.

146. Sub-clause 16D(1) provides that clause 16D applies to organisations that carry on one or more small businesses but do not carry on any other business, and has effect despite clause 16C.

147. Sub-clause 16D(2) delays the application of National Privacy Principles 1, 3 (so far as it relates to the collection of personal information) and 10 to personal information collected by a small business for a period of 12 months after the
commencement of the clause.

148. Sub-clause 16D(3) delays the application of National Privacy Principles 3 (so far as it relates to personal information used or disclosed), 4, 5, 7 and 9 in relation to a small business for a period of 12 months after the commencement of the clause. At the end of the 12 month period, National Privacy Principles 3 (so far as it relates to personal information used or disclosed), 4, 5, 7 and 9 will apply regardless of the time of collection of the personal information by the small business.

149. Sub-clause 16D(4) delays the application of National Privacy Principles 2 and 6 in relation to personal information collected by a small business for a period of 12 months after the commencement of the clause. Sub-clause 16D(5) delays the application of National Privacy Principle 8 in relation to transactions entered into by a small business for a period of 12 months after the commencement of the clause.

150. Clause 16E confirms that the National Privacy Principles do not apply to regulate the handling of personal information by an individual where that information is collected, held, used, disclosed or transferred for personal, family or household affairs (that is, done other than in the course of business). This is consistent with the exemption in sub-clause 7B(1).

151. Clause 16F prohibits the use of personal information collected or held by contracted service providers for the purposes of Commonwealth contract from being used or disclosed for direct marketing unless the use or disclosure is a necessary part of the performance of the contract.

152. Sub-clause 16F(1) specifies the organisations to whom the section applies. It applies to an organisation that is a contracted service provider for a Commonwealth contract and limits the use that can be made of personal information collected for the purpose of meeting, directly or indirectly, an obligation under that contract.

153. Sub-clause 16F(2) prohibits a contracted service provider from using or disclosing the personal information for direct marketing unless the use or disclosure is necessary to meet, directly or indirectly, an obligation under the contract.
154. Sub-clause 16F(3) makes it clear that the prohibition in sub-clause 16F(2) applies despite an approved privacy code that may bind the organisation in relation to the personal information and despite the National Privacy Principles.

155. A heading “Division 4 - Tax File Number Information” is inserted before existing sections 17 and 18 (which relate to tax file number information).

**Item 55. After section 18**

156. Item 55 inserts a heading “Division 5 - Credit Information” before existing sections 18A and 18B (which relate to credit information).

**Item 56. After paragraph 18A(3)(a)**

157. Item 56 inserts a new paragraph 18A(3)(aa). Sub-clause 18A(3) currently lists the matters that the Privacy Commissioner must take into account when preparing a code of conduct relating to credit information files and credit reports. New paragraph 18A(3)(aa) requires the Privacy Commissioner to have regard to the National Privacy Principles and the provisions of Part IIIAA in preparing the code of conduct.
**Item 57. Application**

158. Item 57 confirms that the amendment of section 18A applies to the preparation of the Code of Conduct for issue after the commencement of the amendment.

**Item 58. After Part III**

159. Item 58 inserts a new Part IIIAA. Part IIIAA relates to privacy codes. A privacy code sets out principles for the fair handling of personal information and may be voluntarily adopted by an organisation. The code may or may not set out complaint handling procedures. Where the code does not set out a mechanism for handling complaints, the Privacy Commissioner will be responsible for resolving complaints. Once approved by the Privacy Commissioner and adopted by the organisation, a privacy code replaces the privacy framework provided by the National Privacy Principles.

160. Clause 18BA requires any application to the Privacy Commissioner for approval of a privacy code, to be in writing.

161. Clause 18BB sets out the procedure that the Privacy Commissioner must follow in relation to approving a privacy code. Sub-clause 18BB(1) provides that the Privacy Commissioner may consult any person the Privacy Commissioner considers appropriate before deciding to approve a privacy code. Such consultation may include liaison with enforcement bodies, where the code impacts on the way they are able to perform their functions.

162. Sub-clause 18BB(2) sets out the matters about which the Privacy Commissioner must be satisfied before he or she may decide to approve a privacy code. The code must set out obligations that are at least the equivalent of all the obligations in the National Privacy Principles. The code must specify which organisations are bound by the code (or specify how to determine which organisations are bound by the code). The code must only bind organisations that have consented to be bound by the code, and set out a procedure by which an organisation can cease to be bound by the code.
If the code sets out procedures for making and dealing with complaints, the Privacy Commissioner must have regard to additional factors in sub-clause 18BB(3), and finally, members of the public must have been given an adequate opportunity to comment on a draft of the code.

163. The requirement that an approved privacy code provide at least an equivalent level of privacy protection as the National Privacy Principles will mean that the existence of several codes within an industry is not unduly problematic. The “openness” obligation that an organisation has under National Privacy Principle 5.1 may also be useful in assisting individuals to understand the privacy standards that apply to the organisation with which they are dealing. The code approval process enables industries to set privacy standards above those set out in the National Privacy Principles, particularly where those standards reflect long-standing and strongly held professional values or practices (eg, doctor-patient confidentiality).

164. Sub-clause 18BB(3) sets out the additional matters in paragraphs (a) to (l) about which the Privacy Commissioner must be satisfied in the case where the privacy code sets out procedures for making and dealing with complaints. As part of the process of approving a code the Privacy Commissioner will have to be satisfied that code adjudicators will be required to have due regard for important human rights and social interests which compete with privacy. This provision seeks to ensure that, in performing his or her functions, and exercising his or her powers, a code adjudicator will be required to consider issues such as the general desirability of the free flow of information to the Australian public through the media. This is consistent with the obligation imposed on the Privacy Commissioner under paragraph 29(a).

165. Sub-clause 18BB(4) allows the Privacy Commissioner to consider matters specified in guidelines issued by the Commissioner in deciding whether to approve a privacy code.

166. Sub-clause 18BB(5) provides that the Privacy Commissioner’s approval must be in writing. The Privacy Commissioner’s decision about whether or not to approve a code is not a legislative instrument for the purpose of section 46A of the Acts
Interpretation Act 1901, but it is intended that his or her decisions be judicially reviewable under the Administrative Decisions (Judicial Review) Act 1977.

167. Sub-clause 18BB(6) specifies that the Privacy Commissioner may approve a code that operates for a limited time, or that will expire in certain circumstances, provided the Privacy Commissioner considers that the period or the circumstances are appropriate. An organisation that is no longer bound by a code (because the code has expired, or the organisation has chosen to cease to be bound by it) is, by virtue of new clause 16A, required to refrain from doing an act, or engaging in a practice, that breaches a National Privacy Principle. This means that an organisation cannot evade being subject to privacy standards.

168. Sub-clause 18BB(7) provides that the Privacy Commissioner may still approve a code if it is expressed to apply to all types, or a particular type, of personal information; a specified activity; or a specified industry or profession, or class of industry sectors or professions. An organisation will, to the extent that it is not bound by a privacy code, be required to refrain from doing an act, or engaging in a practice, that breaches a National Privacy Principle.

169. By virtue of clause 18BC, approval of a code will take effect on the day specified in the approval and must not be before the day on which the approval is given.

170. Clause 18BD sets out the procedures for varying an approved privacy code. Sub-clause 18BD(1) requires an application for approval of a variation to be in writing, and sub-clause 18BD(2) requires that the Privacy Commissioner’s approval of a variation also be in writing. In deciding whether or not to approve a variation of a code, sub-clause 18BD(3) requires the Privacy Commissioner to consider all the matters set out in clause 18BB. It is intended that the procedure for approval of a variation be the same as for approval of the code - a code should not escape scrutiny because it introduces something by way of variation rather than at the time it was first approved. The one exception to this is where the variation is minor. In that case, sub-clause 18BD(4) provides that the Privacy Commissioner need not be satisfied that members of the public have been consulted, but may consult any person he or she thinks is
appropriate, instead.

171. The Privacy Commissioner’s approval of a variation takes effect on the day specified in the approval (sub-clause 18BD(5)). Sub-clause 18BD(6) provides that the day specified must not be before the day on which the approval was granted. That is, approval of a variation is not intended to retrospectively validate the acts and practices of an organisation that occurred before the variation of the code was approved.

172. Clause 18BE prescribes the procedures for revoking the approval of a privacy code. The Privacy Commissioner may revoke his or her approval of a privacy code (or variation of a code) on his or her own initiative, or upon an application by an organisation that is bound by the code (sub-clause 18BE(1)). Sub-clause 18BE(2) sets out the consultation procedure the Privacy Commissioner must follow before revoking a code. Any revocation by the Privacy Commissioner must be in writing (sub-clause 18BE(3) and comes into effect on the day specified in the revocation (sub-clause 18BE(4)). The day specified in the revocation must not be before the day on which the revocation is made (sub-clause 18BE(5)).

173. Clause 18BF allows the Privacy Commissioner to make written guidelines:

(a) to assist organisations to develop privacy codes;

(b) relating to making and dealing with complaints under an approved privacy code;

(c) about matters the Privacy Commissioner may consider in deciding whether to approve a privacy code or a variation of a privacy code.

The Privacy Commissioner may publish the guidelines in any way he or she thinks is appropriate.

174. Clause 18BG requires the Privacy Commissioner to keep a register of approved privacy codes.

**Item 59.** After paragraph 27(1)(a)
175. Item 59 inserts new paragraphs 27(1)(aa), (ab) and (ac). Currently, subsection 27(1) lists the functions of the Privacy Commissioner. New paragraphs 27(1)(aa), (ab) and (ac) provide the Privacy Commissioner with additional functions.

176. Paragraph 27(1)(aa) provides the Privacy Commissioner with the function of approving privacy codes and varying or revoking approved privacy codes. Paragraph 27(1)(ab) provides that the Privacy Commissioner has the function, subject to Part V, of investigating an act or practice of an organisation that may be an interference with an individual’s privacy because of clause 13A. This function includes that the Privacy Commissioner may, if he or she considers it appropriate, attempt to effect settlement of the matter giving rise to the investigation, by conciliation. Paragraph 27(1)(ac) provides the Privacy Commissioner with the function of performing functions and exercising powers conferred on an adjudicator under an approved privacy code where the Privacy Commissioner has been appointed as the independent adjudicator under that code.

Item 60.  Paragraph 27(1)(b)

177. Item 60 amends existing paragraph 27(1)(b) by inserting a reference to “organisation”. Currently, paragraph 27(1)(b) describes one of the Privacy Commissioner’s functions as examining proposed legislation that would require or authorise acts or practices which, if done by agencies, might amount to interferences with privacy. The effect of the amendment is to expand the Privacy Commissioner’s focus from acts and practices of agencies to acts and practices of agencies and organisations.

Item 61.  At the end of paragraph 27(1)(d)

178. Item 61 amends existing paragraph 27(1)(d) by inserting a reference to “the National Privacy Principles”. Currently, paragraph 27(1)(d) describes one of the Privacy Commissioner’s functions as promoting an understanding and acceptance of the Information Privacy Principles and their objects. The effect of the amendment is to expand the Privacy Commissioner’s function to promoting an understanding and
acceptance of the National Privacy Principles, as well as the Information Privacy Principles.

**Item 62. Paragraph 27(1)(e)**

179. Item 62 amends existing paragraph 27(1)(e) by inserting a reference to an “organisation”. Currently paragraph 27(1)(e) provides that it is one of the functions of the Privacy Commissioner to publish guidelines in relation to acts or practices of an agency that may interfere with or have an adverse effect on the privacy of individuals. This amendment has the effect of extending the Privacy Commissioner’s guideline publication function to acts and practices of organisations. That is, it is a function of the Privacy Commissioner to publish guidelines in relation to acts or practices of an organisation that may interfere with or have an adverse effect on the privacy of individuals.
Item 63. **After paragraph 27(1)(e)**

180. Item 63 inserts a new paragraph 27(1)(ea) after 27(1)(e), adding three new functions of the Privacy Commissioner to subsection 27(1). Paragraph 27(1)(ea) allows the Privacy Commissioner to make guidelines (and to publish them in a way that he or she considers appropriate) in relation to assisting organisations to develop privacy codes; making and dealing with complaints under an approved privacy code; and matters the Privacy Commissioner may consider in deciding whether to approve a privacy code or a variation of a privacy code.

Item 64. **Paragraph 27(1)(f)**

181. Item 64 repeals paragraph 27(1)(f) and substitutes two new paragraphs 27(1)(f) and (fa). New paragraph 27(1)(f) provides that one of the Privacy Commissioner’s functions is to give advice (with or without a request) to a Minister, agency, organisation or an adjudicator for an approved privacy code on any matter relevant to the operation of the Privacy Act.

182. Paragraph 27(1)(fa) provides details of another function of the Privacy Commissioner, namely, to provide advice (on request) to an adjudicator of an approved privacy code about any matter relevant to the operation of the Act or the privacy code.

Item 65. **Paragraphs 27(1)(n) and (o)**

183. Item 65 repeals paragraphs 27(1)(n) and (o). Paragraph 27(1)(n) described one of the Privacy Commissioner’s functions as encouraging corporations to develop programs for the handling of records of personal information that are consistent with the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines). The National Privacy Principles provide a default privacy framework for the private sector and are consistent with the OECD’s recommendations. Under clause 16A organisations (as defined in subsection 6(1)) are not merely encouraged to develop a
program consistent with the OECD guidelines, they are required to abide by either an approved code (which provides as much privacy protection as the National Privacy Principles) or the National Privacy Principles themselves. Paragraph 27(1)(o) is effectively replaced by new paragraph 27(1)(s), below.

**Item 66. At the end of subsection 27(1)**

184. Item 66 inserts a new paragraph, 27(1)(s), at the end of subsection 27(1). The paragraph replaces old paragraph 27(1)(o), above. New paragraph 27(1)(s) allows the Privacy Commissioner to do anything incidental or conducive to the performance of any of his/her functions.

**Item 67. After subsection 27(1)**

185. Item 67 inserts a new sub-clause 27(1A) after subsection 27(1). New sub-clause 27(1A) provides that the Privacy Commissioner is not subject to Part V of the Act when performing functions or exercising powers as an adjudicator under an approved privacy code. This means that the requirements placed on the Privacy Commissioner to conduct investigations into complaints alleging interferences with privacy and to follow a certain method when conducting an investigation do not apply when the Privacy Commissioner has been appointed as an independent adjudicator under an approved privacy code.

**Item 68. At the end of section 27**

186. Item 68 inserts a new sub-clause 27(3). The effect of the sub-clause is to allow the Privacy Commissioner to examine the records of an organisation in order to ascertain whether the organisation is maintaining its records in accordance with the standards set out in an approved privacy code or, to the extent that the organisation is not bound by an approved privacy code, the National Privacy Principles. The Privacy Commissioner is only able to conduct such an examination if the organisation requests that he or she does so.

**Item 69. Paragraph 29(a)**
187. Item 69 amends paragraph 29(a). Section 29 of the Act sets out those matters which the Privacy Commissioner is required to consider in the performance of his or her functions, and the exercise of his or her powers, under the Act, including the protection of important human rights and social interests that compete with privacy. Some of these competing interests are expressly addressed in the National Privacy Principles, for example, the ability of enforcement bodies to perform their legitimate functions.

188. Currently paragraph 29(a) requires the Privacy Commissioner in making decisions, handling complaints, issuing guidelines and performing other functions to balance the need to ensure proper protection from interferences with privacy against, amongst other things, the general desirability of a free flow of information. The amendment to paragraph 29(a) highlights the important role of the media in the free flow of information to the Australian public. The amendment makes clear that the Privacy Commissioner must have due regard for the general desirability of the free flow of information to the Australian public through the media. This is consistent with the obligation to be imposed on code adjudicators under new paragraph 18BB(3)(c).

**Item 70. Paragraph 29(d)**

189. Item 70 repeals existing paragraph 29(d) and substitutes new paragraph 29(d). This substituted paragraph requires that, in performing his or her functions, and exercising his or her powers, under the Act, the Privacy Commissioner ensures that his or her directions and guidelines are consistent with the Information Privacy Principles, the National Privacy Principles, and the Code of Conduct and Part IIIA, where relevant.

**Item 71. At the end of section 30**

190. Item 71 amends section 30 by adding a new sub-clause 30(6). Currently, section 30 relates to reports to the Minister following an investigation conducted (without a complaint having been made) by the Privacy Commissioner. Subsection 30(1) prescribe the circumstances in which the Privacy Commissioner must report to the
Minister. Sub-clause 30(6) provides that section 30 does not apply to a complaint made under section 36 in relation to an act or practice of an organisation, or a complaint the Privacy Commissioner accepts under sub-clause 40(1B). Sub-clause 40(1B) sets out the circumstances in which the Privacy Commissioner must investigate a complaint made about an organisation even where the organisation is bound by an approved code that contains a complaint handling mechanism. The purpose of sub-clause 30(6) is to clarify that there is no requirement to report to the Minister following investigations conducted by the Privacy Commissioner into the acts and practices of organisations.

**Item 72. Subsection 31(2)**

191. Item 72 amends subsection 31(2). Currently subsection 31(2) describes the circumstances in which the Privacy Commissioner must report to the Minister after the Privacy Commissioner has examined a proposed amendment under paragraph 27(1)(b). Section 27 lists the functions of the Privacy Commissioner. Currently paragraph 27(1)(b) describes one of the Privacy Commissioner’s functions as examining proposed legislation that would require or authorise acts or practices which, if done by agencies, might amount to interferences with privacy. Item 60 of this Bill amends paragraph 27(1)(b) so that the Privacy Commissioner’s focus is expanded from acts and practices of agencies to acts and practices of agencies and organisations. The amendment to subsection 31(2) is consequential to, and consistent with, changes made to paragraph 27(1)(b) by Item 60.

**Item 73. Subsection 36(1)**

192. Item 73 amends subsection 36(1) by requiring that this subsection be read subject to new sub-clause 36 (1A) which is inserted by Item 74.

**Item 74. After subsection 36(1)**

193. Item 74 amends section 36 by inserting new sub-clauses 36(1A), (1B) and (1C) after subsection 36(1). Sub-clause 36(1A) provides that existing subsection 36(1) does not apply in respect of a complaint by an individual about an act or practice of an
organisation that is bound by an approved privacy code which contains a procedure for making and dealing with complaints to an adjudicator in relation to acts and practices that may be an interference with the privacy of an individual, and that is relevant to the act or practice complained of. The effect of this sub-clause, is that an individual may not complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of that individual, if the circumstances in sub-clause 36(1A) apply.

194. Sub-clause 36(1B) provides that sub-clause 36(1A) does not prevent an individual from making a complaint under an approved privacy code to the Privacy Commissioner if the adjudicator, under the code, is the Privacy Commissioner.

195. Sub-clause 36(1C) makes clear that even if an organisation is bound by an approved privacy code that contains a procedure for complaint-handling, an individual may complain to the Privacy Commissioner about an act or practice of an organisation purportedly for the purpose of meeting, directly or indirectly, an obligation under a Commonwealth contract.

**Item 75. Subsection 36(7)**

196. Item 75 repeals subsection 36(7) and inserts new sub-clauses 36(7) and (8).

197. New sub-clause 36(7) provides that where a complaint is made about an act or practice of an organisation, the organisation is to be the respondent to the complaint.

198. Sub-clause 36(8) provides that the respondent to a complaint concerning acts or practices of someone other than an agency or an organisation in relation to tax file number information, data-matching, a breach of guidelines under the *National Health Act 1953*, or a credit reporting infringement, will be the person who engaged in the act or practice.

**Item 76. Application**

199. Item 76 confirms that sub-clause 36(8) applies in relation to complaints made after the commencement of Schedule 1.
Item 77. **Subsection 38(1)**

200. Item 77 amends subsection 38(1) by inserting a reference to “or accepted under subsection 40(1B)” after “36”. Currently, subsection 38(1) describes the conditions under which a representative complaint may be lodged under section 36. This amendment has the effect of extending the conditions under which a representative complaint can be made to complaints accepted by the Privacy Commissioner under sub-clause 40(1B) which is inserted into the Act by Item 80.

Item 78. **Subsection 38(2)**

201. Item 78 amends subsection 38(2) by omitting “under section 36” and substituting “made under section 36 or accepted under subsection 40(1B)”. Currently, subsection 38(2) describes the matters that must be specified in a representative complaint lodged under section 36. This amendment has the effect of extending the requirement for those matters to be specified to complaints accepted by the Privacy Commissioner under sub-clause 40(1B) which is inserted into the Act by Item 80.

Item 79. **Subsection 40(1)**

202. Item 79 amends subsection 40(1) by omitting “The” and substituting “Subject to subsection (1A), the”. This amendment means that it will not be mandatory that the Privacy Commissioner investigate an act or practice that may be an interference with privacy and in respect of which a complaint has been made under section 36, if the circumstances set out in sub-clause 40(1A) apply.

Item 80. **After subsection 40(1)**

203. Item 80 amends section 40 by inserting new sub-clauses 40(1A), (1B) and (1C). Currently, section 40 requires the Privacy Commissioner to investigate acts and practices of agencies and file number recipients that may be interferences with privacy if a complaint is made under section 36. The Privacy Commissioner may, as a matter of discretion, investigate an act or practice that may be an interference with the privacy of an individual, if the Privacy Commissioner thinks it desirable to do so.
204. Sub-clause 40(1A) provides that the Privacy Commissioner must not investigate a complaint if the complainant did not complain to the respondent before approaching the Privacy Commissioner. The Privacy Commissioner may, however, investigate the complaint if it was not appropriate for the complainant to complain to the respondent.

205. Sub-clause 40(1B) allows the Privacy Commissioner to accept a complaint about an act or practice of an organisation bound by an approved privacy code where the complaint is referred to the Privacy Commissioner by the adjudicator under the approved privacy code. If, after consulting the complainant, the Privacy Commissioner accepts the complaint, the Privacy Commissioner must investigate it.

206. Sub-clause 40(1C) provides that, if the Privacy Commissioner accepts a complaint under sub-clause 40(1B), the Privacy Commissioner must deal with it as if it were a complaint made about an act or practice of the organisation under section 36.

Item 81. At the end of section 40

207. Item 81 adds a new sub-clause 40(3) to section 40 which confirms that section 40 has effect subject to section 41.

Item 82. After section 40

208. Item 82 inserts a new clause 40A after section 40. Clause 40A applies where an adjudicator for an approved privacy code forms the view that a complaint is about an act or practice of an organisation that is a contracted service provider for a Commonwealth contract which has been done or engaged in, for the purposes of meeting contractual obligations. The clause provides that despite the code, the adjudicator must stop investigating the complaint under the code without making a determination in relation to the complaint and refer the complaint to the Privacy Commissioner under new sub-clause 40(1B). Sub-clause 40A(3) provides that the Privacy Commissioner must accept the complaint.

Item 83. Subsection 41(1)

209. Item 83 amends subsection 41(1) by inserting “or which the Privacy
Commissioner has accepted under subsection 40(1B)” after “under section 36”. This amendment allows the Privacy Commissioner to decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under sub-clause 40(1B) if any of the situations set out in section 41(1) paragraphs (a) -(f) inclusive are satisfied.

**Item 84. Paragraph 41(1)(b)**

210. Item 84 repeals paragraph 41(1)(b).

**Item 85. Paragraphs 41(1)(e) and (f)**

211. Item 85 repeals paragraphs 41(1)(e) and (f) and replaces them with new paragraphs 41(1)(e) and (f).

212. New paragraph 41(1)(e) provides that the Privacy Commissioner may decide not to investigate, or to further investigate a complaint about an act or practice if satisfied that the act or practice is the subject of an application under another Commonwealth, State or Territory law and the subject-matter of the complaint has been or is being dealt with adequately under that law. The intention of this amendment is to restrict potential forum shopping by complainants.

213. New paragraph 41(1)(f) provides that the Privacy Commissioner may decide not to investigate, or further investigate a complaint about an act or practice, if that act or practice could be made the subject of an application under another Commonwealth, State or Territory law for a more appropriate remedy. The intention of this amendment is to allow the Privacy Commissioner to consider referring complainants to other fora, where appropriate.

**Item 86. Subsections 41(2) and 41(3)**

214. Item 86 amends subsections 41(2) and 41(3). The item inserts “or accepted by the Privacy Commissioner under subsection 40(1B)” after “under section 36” in each subsection. Currently subsection 41(2) provides that the Privacy Commissioner may decide not to investigate a complaint made under section 36 if satisfied that the
complainant has complained to the respondent and the respondent has dealt adequately with the complaint or has not yet had time to deal adequately with the complaint.

215. Subsection 41(3) provides that the Privacy Commissioner may defer the investigation of a complaint under section 36 if the respondent has made an application under section 72 and the Privacy Commissioner is satisfied that deferral of the investigation would not unreasonably prejudice interested persons. This amendment has the effect of extending the Privacy Commissioner’s discretion in subsections 41(2) and 41(3) to investigations of complaints accepted by the Privacy Commissioner under sub-clause 40(1B) which is inserted into the Act by Item 80.

Item 87. Subsection 41(4)

216. Item 87 repeals subsection 41(4) and replaces it with new sub-clause 41(4). Subsection 41(4) relates to investigating acts or practices which may breach Information Privacy Principle 7 which deals with correction of personal information. New sub-clause 41(4) extends the provision to include investigating acts or practices under National Privacy Principle 6 or a provision of an approved privacy code to the extent that they deal with correction of personal information.

Item 88. Section 42

217. Item 88 amends section 42. The item inserts “or the Commissioner accepts a complaint under subsection 40(1B)” after “Commissioner” (first occurring). Currently, section 42 provides that when a complaint is made the Privacy Commissioner may make preliminary inquiries of the respondent to determine whether the Privacy Commissioner has the power to investigate further or whether the Privacy Commissioner should decide not to investigate the matter. This amendment has the effect of extending the ability of the Privacy Commissioner to make preliminary inquiries to where a complaint has been accepted under sub-clause 40(1B) which is inserted into the Act by Item 80.

Item 89. After subsection 43(1)
218. Item 89 inserts a new sub-clause 43(1A). This sub-clause facilitates the accountability of contracted service providers to the agency to whom the service is being provided under a Commonwealth contract. The new sub-clause requires the Privacy Commissioner to inform the relevant agency that the act or practice of a contracted service provider is to be investigated before commencing the investigation.

**Item 90. Subsection 43(6)**

219. Item 90 amends subsection 43(6) by inserting a reference to “organisation” after “agency” (twice occurring). Currently, subsection 43(6) provides that the Privacy Commissioner may allow an agency or person appearing before the Privacy Commissioner to make a submission under subsection 43(5) to be represented by another person. This amendment will have the effect of permitting the Privacy Commissioner to allow an organisation appearing before the Privacy Commissioner to make a submission under subsection 43(5) to be represented by another person.

**Item 91. After subsection 43(8)**

220. Item 91 inserts a new sub-clause 43(8A) into section 43. New sub-clause 43(8A) limits the Privacy Commissioner’s discretionary power in existing subsection 43(8) to discuss any matter that is relevant to the investigation of a complaint under Division V with a Minister. This provision states that subsection 43(8) does not allow the Privacy Commissioner to discuss a matter relevant to an investigation of a breach of the National Privacy Principles or an approved code unless it concerns an act done by, or practice engaged in, by a contracted service provider for a Commonwealth contract and for the purpose of providing a service to an agency to meet contractual obligations.

**Item 92. Subsection 46(1)**

221. Item 92 amends subsection 46(1) by inserting “(except an NPP complaint or a code complaint accepted under subsection 40(1B))” after “a complaint”. Currently, subsection 46(1) provides that in the course of performing functions in relation to a complaint, the Privacy Commissioner may give written notice to direct persons to
attend, at a time and place specified in the notice, a conference presided over by the Privacy Commissioner. This amendment will have the effect of preventing the Privacy Commissioner from directing persons to attend a conference in relation to complaints concerning the National Privacy Principles or a complaint accepted under sub-clause 40(1B) which is inserted into the Act by Item 80.

**Item 93. At the end of section 48**

222. Item 93 adds a new sub-clause 48(2). Section 48 currently requires the Privacy Commissioner to inform the complainant and the respondent of, and the reasons for, a decision not to investigate, or not to investigate further, a matter to which a complaint relates. New sub-clause 48(2) provides that if the Privacy Commissioner decides not to investigate an act or practice of a contracted service provider, either at all or after commencing an investigation, the Privacy Commissioner must also inform the agency of the decision.

**Item 94. After section 50**

223. Item 94 adds a new clause 50A after section 50. Clause 50A allows the Privacy Commissioner to substitute an agency for an organisation as respondent to a complaint. Sub-clause 50A(1) sets out when the Privacy Commissioner may use this power. (It only applies if the organisation is a contracted service provider for a Commonwealth contract to provide services to the agency.) Substitution may be made before the Privacy Commissioner has made a determination in relation to the complaint if the contracted service provider is not available or appropriate as respondent for one of the reasons specified. Should the Privacy Commissioner consider it appropriate to do so, new sub-clause 50A(2) allows the Privacy Commissioner to amend a complaint to substitute the agency, or the principal executive of the agency, as respondent to a complaint. The ability of the Privacy Commissioner to substitute an agency as respondent ensures that an individual complainant does not suffer loss in the event that the respondent contracted service provider has become insolvent, commenced to be wound up or ceased to exist for other similar reasons.
224. New sub-clause 50A(3) provides that before the Privacy Commissioner amends a complaint in this way he or she is required to give the agency a notice informing the agency of the proposed amendment to the complaint and giving reasons for the proposed amendment. The Privacy Commissioner must then provide to the agency an opportunity to make oral and/or written submissions to the Privacy Commissioner concerning the proposed amendment.

225. Under new sub-clause 50A(4), if the Privacy Commissioner has already started investigating a complaint under section 40 before it is amended to substitute the agency for the contracted service provider, the Privacy Commissioner is taken to have informed the outsourcing agency that the matter is to be investigated, to satisfy the requirements of sub-clause 43(1A).

**Item 95. Subsection 52(3A)**

226. Item 95 repeals subsection 52(3A) and inserts new sub-clauses 52(3A) and (3B). Sub-clause 52(3A) provides that the Privacy Commissioner may include an order of the kind set out in sub-clause 52(3B) in a determination made under subparagraph 52(1)(b)(i) or (ii) that concerns a breach of the relevant Information Privacy Principle, National Privacy Principle, provision of an approved privacy code, or credit reporting provision that deals with the correction of personal information.

227. Sub-clause 52(3B) sets out the orders that may be included in the determination made under subparagraph 52(1)(b)(i) or (ii). They are that the agency or respondent correct, delete or add to a record, credit file or credit report; or that the agency or respondent attach a statement provided by the complainant to the record, credit file or credit report seeking correction, deletion or addition.

**Item 96. At the end of Division 2 of Part V**

228. Item 96 adds new clauses 53A and 53B at the end of Division 2 of Part V. Like the amendment inserted by Item 95, clause 53A adds a requirement for notification, should the Privacy Commissioner make a determination to which a contracted service provider is the respondent. The clause provides that the Privacy Commissioner must
give a copy of the determination to each agency to which services are or were to be provided under the Commonwealth contract, if the Privacy Commissioner considers it appropriate. After consultation with any such agency, the Privacy Commissioner may recommend to such an agency any measures the Privacy Commissioner considers appropriate. Within 60 days of receiving the recommendation, the outsourcing agency must inform the Privacy Commissioner of any action that it proposes to take concerning the recommendation.

229. Item 96 also inserts new clause 53B, which applies if the respondent to a determination under subsection 52(1) is a contracted service provider for a Commonwealth contract and the determination includes a declaration that the complainant is entitled to a specified amount by way of compensation or reimbursement. The clause only applies if the contracted service provider is not available or appropriate as respondent to the determination for one of the reasons specified. The new clause allows the Privacy Commissioner to make a determination in writing that a specified agency to which services were or were to be provided under the contract is taken to be the respondent in relation to the determination. This will ensure that the individual complainant does not suffer loss in the event that the contracted service provider is not able to provide compensation or pay costs awarded, for one of these reasons. Before the Privacy Commissioner makes such a determination the Privacy Commissioner is required to give the relevant agency a notice informing the agency of the proposed determination and giving reasons for the proposal. The Privacy Commissioner must give the agency an opportunity to make oral and/or written submissions to the Privacy Commissioner concerning the proposed determination.

**Item 97. Division 3 of Part V (heading)**

230. Item 97 repeals the heading and replaces it with “Division 3 - Enforcement”.

**Item 98. After subsection 54(1)**

231. Item 98 inserts a new sub-clause (1A) into section 54. The purpose of the
amendment is to extend the application of Division 3 of Part V to determinations made by an adjudicator for an approved code under the code in relation to a complaint under the code.

**Item 99. Section 55**

232. Item 99 repeals section 55 and substitutes new clauses 55, 55A and 55B.

233. Clause 55 confirms that an organisation that is a respondent to a determination made by the Privacy Commissioner under section 52, or a determination made by an adjudicator under an approved privacy code, must not repeat the conduct identified in the determination as being an interference with privacy, and must perform any act or course of conduct that is specified in the determination.

234. Clause 55A relates to proceedings in the Federal Court or Federal Magistrates Court to enforce a determination. Sub-clause 55A(1) provides that proceedings in either court may be commenced by the complainant, the Privacy Commissioner (if the determination was made under section 52), or the adjudicator for an approved privacy code (if the determination was made by him or her under an approved privacy code). The court may, if it thinks fit, grant an interim injunction pending the determination of the proceedings (sub-clause 55A(3)) but can not require a person to give undertakings as to damages (sub-clause 55A(4)).

235. If the court is satisfied, by way of hearing *de novo* (sub-clause 55A(5)), that the respondent has engaged in conduct that constitutes an interference with the privacy of the complainant, the court may make such orders (including a declaration of right) as it thinks fit (sub-clause 55A(2)). Sub-clauses 55A(6) and (7) provide that, in hearing the matter, the court may receive into evidence: a copy of the written reasons for the determination, a copy of any document that was before the decision maker, and a copy of a record of any appearance before the decision maker.

236. Clause 55B relates to evidentiary certificates. Sub-clauses 55B(1) and (2) provide that a certificate may be issued by the Privacy Commissioner, or an adjudicator for an approved privacy code, setting out the findings of fact upon which
he or she based his or her determination that a specified body (i.e., an agency or organisation) had breached the relevant privacy standard (i.e., Information Privacy Principles in the case of an agency, or National Privacy Principles or approved code in the case of an organisation).

237. Sub-clause 55B(3) provides that the certificate is *prima facie* evidence of the facts found by the Privacy Commissioner or adjudicator, but not prima facie evidence of a finding that an agency or organisation had breached the relevant privacy standard (because the question of whether a breach has occurred is a question the court must consider *de novo*). A document purporting to be a certificate must be taken to be a certificate unless the contrary is established (sub-clause 55B(4)). The purpose of the certificate is to facilitate the enforcement process.

**Item 100. Application**

238. Item 100 provides that Division 3 of Part V, as amended, applies to determinations made as a result of a complaint that is made *after* the commencement of the Schedule. Clause 55B applies in relation to determinations made by the Privacy Commissioner in relation to an agency *before* or *after* the commencement of the clause.

**Item 101. Subsections 62(1) and (2)**

239. Item 101 amends subsections 62(1) and (2). The item inserts “or the Federal Magistrates Court” after “Federal Court” in both subsections. Currently subsection 62(1) states that where an agency fails to comply with section 58 (which sets out the obligations of a respondent agency), an application may be made to the Federal Court for an order directing the agency to comply. Similarly, subsection 62(2) states that where the principal executive officer of an agency fails to comply with section 59 (which sets out the obligations of a principal executive officer of an agency), an application may be made to the Federal Court for an order directing the principal executive to comply. Item 101 amends subsection 62(1) and 62(2) so that an application may be made to the Federal Magistrates Court as well as to the Federal
Item 102. Subsection 62(4)

240. Item 102 amends subsection 62(4). The item substitutes the word “court” for “Federal Court”. Currently, subsection 62(4) provides that, on application under section 62, the Federal Court may make such orders as it sees fit to secure the compliance of the respondent. This amendment will have the effect of broadening subsection 62(4) to allow either the Federal Court or the Federal Magistrates Court, on application, to make such orders as they see fit to secure the compliance of the respondent.

Item 103. Paragraphs 63(2)(a) and (b)

241. Item 103 amends paragraphs 63(2)(a) and (b). The item inserts “or the Federal Magistrates Court” after “Federal Court” in both paragraphs. Currently, paragraphs 63(2)(a) and (b) provide that a person who has commenced proceedings in the Federal Court under section 55, or has been involved in proceedings commenced in the Federal Court under section 55 as a result of their alleged conduct, may apply to the Attorney-General for assistance in respect of those proceedings. This amendment will have the effect of broadening the paragraphs to allow a person to apply to the Attorney-General for assistance where the relevant proceedings have been commenced in the Federal Magistrates Court under clause 55A.

Item 104. After subsection 63(2)

242. Item 104 inserts a new sub-clause 63(2A) after subsection 63(2). Sub-clause 63(2A) prohibits the making of an application for legal assistance in relation to enforcement proceedings relating to a code complaint or an NPP complaint.

Item 105. At the end of section 64

243. Item 105 inserts new sub-clause 64(2) at the end of section 64. Sub-clause 64(2) protects an adjudicator for an approved privacy code, or any person acting under his or her direction or authority, from legal proceedings arising from an act done under this
Bill, or the approved privacy code, that was performed in good faith.

**Item 106. After subsection 66(1)**

244. Item 106 inserts new sub-clause 66(1A), after subsection 66(1). Subsection 66(1) makes it an offence for a person to refuse or fail to give information, to answer a question, or produce a document or record, when required to do so under the Act, without reasonable excuse.

245. New sub-clause 66(1A) provides that a journalist has a reasonable excuse if giving the information, answering a question or producing a document or record would tend to reveal the identity of a person who gave information to the journalist in confidence. This provision is intended to assist in balancing the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media.

**Item 107. After paragraph 67(a)**

246. Item 107 inserts new paragraphs (aa) and (ab) after paragraph 67(a). Paragraphs 67(aa) and (ab) preclude a person from being sued for lodging a complaint under an approved privacy code or for the acceptance by the Privacy Commissioner of a complaint under sub-clause 40(1B), respectively.

**Item 108. Subsection 68(1)**

247. Item 108 amends section 68(1) to insert the words “in writing” after “Commissioner”. This requires that a person authorised by the Privacy Commissioner to enter premises under section 68 must be so authorised in writing by the Privacy Commissioner.

**Item 109. Subsection 68(1)**

248. Item 109 amends subsection 68(1) to include a reference to “an organisation” after “an agency”. This amendment allows the Privacy Commissioner to authorise a person to enter premises occupied by an organisation.
Item 110.  **After subsection 68(1)**

249. Item 110 inserts a new sub-clause 68(1A) into subsection 68(1). Sub-clause 68(1A) provides that a person may be authorised to enter premises under section 68 only while the person is a member of the staff assisting the Privacy Commissioner.

Item 111.  **After subsection 68(3)**

250. Item 111 inserts new sub-clauses 68(3A), (3B), (3C) and (3D) into subsection 68(3). Sub-clause 68(3A) provides that a person authorised under subsection 68(1) to enter premises must inform the occupier or person in charge that he or she may refuse to consent to the entry by the authorised person.

251. Sub-clause 68(3B) provides that, if consent given to the authorised person is not voluntary (for example, if a person authorised under subsection 68(1) fails to comply with sub-clause 68(3A)), then the entry is unlawful.

252. Sub-clause 68(3C) requires that an authorised person must produce his or her identity card (as defined in clause 68A (Item 112) on request by the occupant or person in charge. Sub-clause 68(3D) requires that the authorised person leave the premises if so requested by the occupier or person in charge.

Item 112.  **After section 68**

253. Item 112 inserts new sub-clauses 68A(1), (2) and (3) after section 68. Sub-clause 68A(1) requires that the Privacy Commissioner issue persons authorised under section 68 to enter premises with an identity card containing a recent photograph of the authorised person. Sub-clause 68A(2) provides that, as soon as practicable after a person ceases to be so authorised, he or she return the identity card to the Privacy Commissioner. Sub-clause 68A(3) provides that if sub-clause 68A(2) is contravened, one penalty unit is imposed.

Item 113.  **Subsection 69(9) (definition of complaint)**

254. Item 113 repeals the existing definition of “complaint” in subsection 69(9) and
substitutes a new definition of “complaint”. Item 113 defines “complaint”, for the purposes of section 69, to mean a complaint under section 36 or a complaint the Privacy Commissioner accepts under sub-clause 40(1B).

**Item 114. At the end of Division 5 of Part V**

255. Item 114 inserts new sub-clauses 70A(1), (2) and (3) at the end of Division 5 of Part V. These sub-clauses deal with the situation where Part V imposes an obligation on an entity that does not have separate legal personality, namely a partnership, unincorporated association or trust.

256. Sub-clause 70A(1) provides that, where Part V imposes an obligation on an organisation that is a partnership, this obligation is imposed on each partner individually and may be discharged by any of the partners to the partnership.

257. Sub-clause 70A(2) provides that, if Part V imposes an obligation on an unincorporated association, the obligation is imposed on each member of the committee of management of the association and may be discharged by any member of that committee.

258. Sub-clause 70A(3) provides that if Part V imposes an obligation on a trust, the obligation is imposed on each trustee but may be discharged by any one of the trustees.

**Item 115. Part VI (heading)**

259. Item 115 repeals the heading “Part VI - Public interest determinations about certain acts and practices” and substitutes “Part VI - Public interest determinations and temporary public interest determinations”.

**Item 116. Before section 71**

260. Item 116 inserts a new heading “Division 1 - Public Interest Determinations” before section 71.

**Item 117. Section 72**
261. Item 117 omits the reference to “Part” in section 72 and substitutes “Division” to reflect the changes made by Item 116.

**Item 118. At the end of section 72**

262. Item 118 adds new sub-clauses 72(2), (3), (4) and (5). Sub-clause 72(2) provides that the Privacy Commissioner may make a written determination that an act or practice of an organisation which is in breach, or may be in breach, of an approved privacy code, or a National Privacy Principle, that binds the organisation, is not to be regarded as a breach of the code or National Privacy Principle because of the overriding public interest in the organisation being able to do the act, or engage in the practice.

263. A determination under sub-clause 72(2) applies only to acts or practices that occur while it is in force. Sub-clause 72(3) provides that the effect of a determination under sub-clause (2) is that the organisation is taken not to contravene clause 16A (which provides that an organisation must comply with the National Privacy Principles or an approved privacy code). Sub-clause 72(4) provides that the Privacy Commissioner may make a written determination that applies a determination made under sub-clause (2) generally to all organisations. Sub-clause 72(5) provides that a determination under sub-clause (4) which gives determinations under sub-clause (2) general effect, is to have effect according to its terms.

**Item 119. Subsection 73(1)**

264. Item 119 inserts “or organisation” after the word “agency” in subsection 73(1). This allows an organisation to apply, in accordance with any regulations, for a public interest determination under section 72 about an act or practice.

**Item 120. At the end of subsection 73(1)**

265. Item 120 inserts “of the agency or organisation” at the end of subsection 73(1). This allows an agency or organisation to seek a public interest determination in respect of an act or practice of the agency or organisation.
Item 121. Subsection 73(2)

266. Item 121 substitutes the term “services” for “care” in subsection 73(2). This amendment is not intended to substantively change the operation of subsection 73(2). It is intended to ensure consistency in the terminology used in the Act. A “health service” is a term that is defined in Item 17 of the Bill.

Item 122. Subsection 75(2)

267. Item 122 repeals subsection 75(2) and inserts new sub-clauses 75(2) and (2A). Sub-clause 75(2) provides that, if the applicant for a public interest determination is an agency then the Privacy Commissioner must send a written invitation to the agency and any other person interested in the application to notify him or her if the agency or other person wishes the Privacy Commissioner to hold a conference about the draft determination. Sub-clause 75(2A) provides that, if the applicant for a public interest determination is an organisation, the Privacy Commissioner must send a written invitation to the organisation to notify him or her within a specified time whether the organisation wishes the Privacy Commissioner to hold a conference about the draft determination. Sub-clause 75(2A) also requires that the Privacy Commissioner issue, in any way he or she considers appropriate, an invitation in similar terms to any other persons the Privacy Commissioner thinks appropriate.

Item 123. Subsection 75(3)

268. Item 123 inserts the words “or subsection (2A)” after the words “subsection (2)” in subsection 75(3). This is to reflect that an invitation must also be made under sub-clause (2A).

Item 124. Application and saving

269. Sub-item 1 of Item 124 provides that the amendments of section 75 made by Items 103 and 104 apply only in relation to applications made under section 73 after the commencement of this Schedule. Sub-item 2 provides that any regulations in force before commencement of the Schedule continue to have effect as if they had been
made for the purposes of that subsection after that commencement. Sub-item 3 provides that sub-item 3 does not prevent amendment or repeal of regulations that are in force before commencement of this Schedule.

**Item 125. Subsection 76(1)**

270. Item 125 inserts “organisation” after “agency” wherever it occurs in subsection 76(1). This allows an organisation to request a conference about a draft determination.

**Item 126. Subsection 76(4)**

271. Item 126 inserts “organisation” after “agency” in subsection 76(4). This amendment extends the application of the current subsection 76(4) to cover the circumstance where an organisation requests that the Privacy Commissioner hold a conference about a draft determination and requires the Privacy Commissioner to give notice of the day, time and place of the conference to the organisation.

**Item 127. Subsection 77(1)**

272. Item 127 inserts “or organisation” after “agency” wherever it occurs in subsection 77(1). This extends the coverage of subsection 77(1) to entitle an organisation to be represented at a conference about a draft determination by a person who is, or persons each of whom is, an officer or employee of the organisation.

**Item 128. Subsection 79(2)**

273. Item 128 substitutes “organisation or any other person” for “or any person” in subsection 79(2). Subsection 79(2), requires that the Privacy Commissioner take account of all submissions about an application for a draft determination whether at the conference or not, by the agency or any other person. This amendment by Item 128 also requires that the Privacy Commissioner take account of any submission made by the organisation making the application.

**Item 129. At the end of Part VI**

274. Item 129 inserts new Division 2 – Temporary public interest determinations,
comprising clauses 80A, 80B, 80C, 80D, and Division 3 – Register of determinations comprising clause 80E.

275. Sub-clause 80A(1) provides that the Privacy Commissioner may issue a temporary public interest determination in respect of an act or practice of an agency or organisation that breaches or may breach an Information Privacy Principle (in respect of agencies) or an approved privacy code or a National Privacy Principle (in respect of organisations) and is the subject of an application by either an agency or organisation under section 73 for a public interest determination under section 72. The power to issue temporary public interest determinations is restricted by paragraphs (b) and (c) of sub-clause 80A(1) to circumstances requiring an urgent decision and where the Privacy Commissioner is satisfied that the public interest in the agency or organisation continuing to perform the act, or engage in the practice, outweighs to a substantial degree, the public interest in adhering to the relevant Principle or code.

276. Sub-clause 80A(2) provides that the Privacy Commissioner may make a written temporary public interest determination noting that he or she is satisfied of the matters set out in sub-clause 80A(1). This may be done either at the request of any agency or organisation or on his or her own initiative.

277. Sub-clause 80A(3) provides that the temporary public interest determination must specify the time period (not being more than 12 months) during which the determination is in force (subject to sub-clause 80A (2)) and include a statement of reasons for the determination.

278. Sub-clause 80B(1) provides that an act or practice of any agency that is the subject of a temporary public interest determination will not breach section 16 if that act is done or practice engaged in, while the determination is in force.

279. Sub-clause 80B(2) provides that an act or practice of any organisation that is the subject of a temporary public interest determination will not breach section 16 if that act is done or practice engaged in, while the determination is in force.

280. Sub-clause 80B(3) provides that the Privacy Commissioner may make a written
determination which effectively extends the effect of a temporary public interest determination made in respect of the act or practice of one organisation, to apply to any organisations and not just the organisation in respect of which the determination was made. Sub-clause 80B(4) provides that a determination has effect according to its terms.

281. Clause 80C provides that a determination made under new Division 2, is a disallowable instrument for the purposes of section 46A of the Acts Interpretation Act 1901.

282. Sub-clause 80D(1) provides that the making of a determination under new Division 2 does not prevent the Privacy Commissioner from dealing with an application for a public interest determination under section 73 in respect of that act or practice.

283. Sub-clause 80D(2) sets out the circumstances in which a determination about an act or practice under new Division 2 ceases to have effect. A temporary public interest determination will cease to have effect where a public interest determination under subsection 72(1) or (2) about the act or practice comes into effect or where a determination is made under paragraph 78(b) by the Privacy Commissioner to dismiss the application for a determination.

284. Sub-clause 80E(1) requires that the Privacy Commissioner keep a register of determinations made under Division 1 or 2. This will require the Privacy Commissioner to maintain a list of public interest determinations made in respect of agencies or organisations (section 72), temporary public interest determinations under sub-clause 80A(2) and determinations that give a temporary public interest determination general effect under sub-clause 80B(3).

285. Sub-clause 80E(2) allows the Privacy Commissioner to determine the form of the register and how it is to be kept. Sub-clause 80E(3) requires the Privacy Commissioner to make the register publicly available in a way that the Privacy Commissioner determines. This may be via the World Wide Web or any other means
allowing the public to access current determinations made by the Privacy Commissioner. Sub-clause 80E(4) provides that the Privacy Commissioner may charge fees for making the register available to the public or providing copies of, or extracts from, the register.

Item 130. Application

286. Item 130 provides that clause 80A applies in respect of an application made by or on behalf of any agency under section 73 regardless whether the application was made before or after the commencement of the Bill. An application made by an agency under section 73 before the commencement of this Schedule may therefore be the subject of a temporary public interest determination once clause 80A commences, notwithstanding that the application was made before clause 80A commenced.

Item 131. After section 95

287. Item 131 inserts new clauses 95A, 95B and 95C.

288. Sub-clause 95A(1) allows the Privacy Commissioner to approve, for the purposes of the National Privacy Principles, guidelines issued by the National Health and Medical Research Council or a “prescribed authority” about specified aspects of the handling of health information. A “prescribed authority” is an authority prescribed by the Governor-General under the existing regulation-making power in the Act.

289. Under sub-clause 95A(2), the Privacy Commissioner may approve guidelines relating to the use and disclosure of health information for the purposes of research, or the compilation or analysis of statistics, aimed at improving public health or public safety. The approval of guidelines is to be evidenced by notice in the Gazette.

290. Under sub-clause 95A(3), the “test” for approval is that the public interest in the use or disclosure of health information for public health or public safety purposes in accordance with the guidelines substantially outweighs the public interest in maintaining the level of privacy protection afforded by the National Privacy Principles (other than paragraph 2.1(d)).
291. Sub-clause 95A(4) provides that the Privacy Commissioner may approve guidelines relating to the collection of health information for the purposes set out in National Privacy Principle 10.3.

292. Under sub-clause 95A(5) the “test” for approval of such guidelines is that the public interest in the collection of health information for National Privacy Principle 10.3 purposes in accordance with the guidelines substantially outweighs the public interest in maintaining the level of privacy protection afforded by the National Privacy Principles (other than paragraph 10.3(d)). Under sub-clauses 95A(3) and (5), the “level of privacy protection” is to be judged at the time the Privacy Commissioner is considering whether to approve the guidelines.

293. Sub-clause 95A(6) provides that the Privacy Commissioner may revoke an approval of guidelines, if he or she is no longer satisfied of the matter that he or she had to be satisfied of to approve the guidelines. This sub-section would permit, for example, a revocation of the approval of guidelines in circumstances where the guidelines are out-of-date. The Privacy Commissioner’s approval of updated guidelines would need to meet the relevant “test” for approval in either sub-clauses 95A(3) or (5).

294. Sub-clause 95A(7) provides that an application may be made to the Administrative Appeals Tribunal for review of a decision of the Privacy Commissioner to refuse to approve guidelines, or to revoke an approval of guidelines.

295. New clause 95B requires an agency to consider its own obligations under the Act when entering into a Commonwealth contract. It requires an agency to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done by the agency. The obligation on the agency to ensure that the contract does not authorise a contracted service provider to do such an act or engage in such a practice also extends to ensuring that such an act or practice is not authorised by a subcontract. The section applies to agencies entering into Commonwealth contracts in their own right as well as those entering a contract on behalf of the
Commonwealth.

296. To ensure that individuals can find out about the content of privacy clauses agreed between agencies and organisations and included in Commonwealth contracts, clause 95C enables a person to ask a party to the contract for this information. The clause requires the party requested to inform the person, in writing, of the content of any provisions in the contract (if any) that are inconsistent with an approved code binding a party to the contract or with a National Privacy Principle. For example, the contract may contain a provision concerning the contractor’s ability to use or disclose personal information that is not consistent with National Privacy Principle 2. If asked, a party to the contract would be required to inform the person of the content of that provision. This ensures that parties to a Commonwealth contract cannot claim “commercial-in-confidence” in respect of privacy standards contained in Commonwealth contracts, thereby preserving accountability and openness in respect of these standards.

Item 132. Subsection 97(2)

297. Item 132 omits the words “27(1)(n)” from subsection 97(2). This amendment is a consequential amendment arising from the amendments made by Item 65, which repeals paragraph 27(1)(n).

Item 133. After subsection 97(2)

298. Item 133 inserts new sub-clause 97(2A) after subsection 97(2). This requires that the annual report which the Privacy Commissioner must provide to the Minister include a statement about the operation of approved privacy codes that contain procedures for making and dealing with complaints in relation to acts or practices that may be an interference with the privacy of an individual. This statement must include action taken by adjudicators to monitor compliance with codes and the number of complaints made under approved privacy codes and their nature and outcome.

Item 134. Subsections 98(1) and (2)
299. Item 134 inserts “or the Federal Magistrates Court” after “Federal Court”. This recognises that the Federal Magistrates Court has jurisdiction to grant injunctions restraining conduct that constituted or would constitute a contravention of the Act.

Item 135. Subsections 99A(1) and (2)

300. Item 135 omits “servant” (wherever occurring) in subsections 99A (1) and (2) and substitutes “employee”. This amendment recognises that section 99A now applies to organisations as well as to agencies. Subsection 99A(1), as amended, provides that, in proceedings for an offence against the Act where it is necessary to establish the state of mind of a body corporate in relation to particular conduct, it will be sufficient to show that the director, employee, or agent of the body corporate had the requisite state of mind (provided that the conduct was engaged in by the person within the scope of his or her authority).

301. Subsection 99A(2) provides that conduct that is within the scope of the director’s, employee’s or agent’s authority and engaged in on behalf of a body corporate by that person is to be taken, for the purposes of prosecution of an offence against the Act, to have been conduct engaged in also by the body corporate.

302. The heading to section 99A is consequentially amended by omitting “servants” and substituting “employees”.

Item 136. Paragraph 99A(3)(a)

303. Item 136 omits “a servant” and substitutes “an employee” in paragraph 99A(3)(a). Like the amendments to subsections 99A(1) and (2), this amendment reflects the extension of subsection 99A(3) to cover organisations as well as agencies.

Item 137. Paragraph 99A(3)(b)

304. Item 137 omits “servant” and substitutes “employee” in paragraph 99A(3)(b). Amended subsection 99A(3) provides that, in proceedings for an offence against the Act, where it is necessary to establish the state of mind of a person other than a body corporate in relation to particular conduct, it is sufficient to show that the conduct was
engaged in by an employee or agent within the scope of his or her authority and that the person had that particular state of mind.

**Item 138. Subsection 99A(4)**

305. Item 138 omits “a servant” and substitutes “an employee” in subsection 99A(4). Amended subsection 99A(4) provides that conduct engaged in on behalf of a person other than a body corporate by an employee or agent of that person (within the scope of that person’s actual or apparent authority) is to be taken, for the purposes of a prosecution for an offence against the Act, to have been engaged in also by the first mentioned person, unless that person can establish that he or she took reasonable precautions and exercised due diligence to avoid the conduct.

**Item 139. At the end of the Act**

306. Item 139 inserts Schedule 3 “National Privacy Principles”.

307. The National Privacy Principles (NPPs) relate to fair handling of personal information and set the standards for the private sector. They apply to private sector organisations that do not have their own privacy codes that have been approved by the Privacy Commissioner. The NPPs apply to personal information collected, held, used or disclosed by an organisation. To remove doubt, a reference to “law” in the NPPs means Commonwealth, State and Territory legislation, as well as the common law.

**Principle 1 - collection**

308. The reference in the NPPs to the collection of personal information by organisations means, by virtue of clause 16B, a reference to collection of that information for inclusion in a record or generally available publication. (That is, the NPPs regulate the collection of personal information to the extent that the information is collected for inclusion in a record or generally available publication.) Where an organisation has already collected the personal information, the NPPs apply only to the extent that the information is held by the organisation in a record.

309. **NPP 1.1** provides that personal information must not be collected by an
organisation unless the information is necessary for one or more of its functions or activities. ‘Necessary’ should be interpreted in a practical sense. If an organisation cannot, in practice, effectively pursue a function or activity without collecting personal information, then that personal information would be regarded as necessary for that function or activity. An organisation should not collect personal information on the off chance that it may become necessary for one of its functions or activities in the future. If an organisation receives personal information that is not necessary for one of its functions or activities, it should not retain that personal information.

310. NPP 1.2 provides that an organisation must collect information only by lawful and fair means and not in an unreasonably intrusive way. ‘Lawful means’ refers to methods that are not prohibited by law. ‘Fair’ means without intimidation or deception. This would usually require organisations not to collect personal information covertly but there will be some circumstances - for example, investigations of possible fraud or other unlawful activity - where covert collection of information by surveillance or other means would be fair.

311. NPP 1.3 provides that when collecting personal information about an individual from that individual, the organisation collecting the information must, at or before the time of collection (or, if that is not practicable, as soon as practicable after), take reasonable steps to ensure that the individual is aware of the identity of the organisation and how to contact it, the fact that the individual is able to gain access to the information, the purposes for which the information is collected, the disclosure practices of the organisation in relation to the information, any law that requires the particular information to be collected and the consequences (if any) for the individual if the information is not provided.

312. Where information is being collected on a form, an organisation’s obligations under 1.3 could be satisfied by a statement on the form. Where information is collected via the internet, NPP 1.3 would require that a policy statement appear on the web page notifying the individual of contact details of the organisation collecting the information and outlining in what circumstances, and for what purposes personal
information (such as an email address, name or other personal details including purchasing habits linked to an email address) is collected. The Privacy Commissioner has prepared Guidelines on email and web-browsing.

313. In relation to the requirement in 1.3(c) to tell the individual the purposes for which the information is collected: The description of the purposes may be kept reasonably general, and internal purposes that form part of normal business practice need not be mentioned. If the collection is made for only one purpose, it would often be apparent simply from the title of a form, for example, ‘Application for Membership’. Informing an individual about the purposes of collection will often assist the individual to understand the types of persons within an organisation that may be handling his or her personal information. It will also be of assistance in defining how personal information may be used or disclosed under NPP 2.1.

314. In relation to the requirement in 1.3(d) to tell the individual about the types of organisations to which the organisation usually discloses information of the kind collected from the individual: ‘Reasonable steps’, in this context, means giving generic descriptions of sets of organisations (eg, ‘debt collectors’ or ‘State Government licensing authorities’ or ‘health insurers’) where it is not practicable to list each member of the set. Disclosures that may happen but in practice happen only rarely - like disclosures under warrant or to intelligence agencies - would not need to be mentioned. If an organisation is a member of a group of related bodies corporate, it would be appropriate for an organisation to let the individual know that his or her personal information may be given to bodies corporate that are related to that organisation.

315. In relation to the requirement in 1.3(e) to tell the individual about any law that requires the information to be collected: This paragraph is intended to cover any legal obligation to provide the information or any legal obligation on the organisation to collect it. In describing such an obligation, it would be desirable to specify the exact piece of legislation that imposes the obligation (where it is feasible to do so).

316. In relation to the requirement in 1.3(f) to tell the individual about the
consequences of not providing personal information: An organisation would not be required to try to describe all possible consequences of not providing information, but should make it clear which items are essential to fulfil the purpose of collection and which are not.

317. **NPP 1.4** notes that as a general rule, and if it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual. There will, however, be situations in which it would not be ‘reasonable and practicable’ to collect directly from an individual. An example would be where direct collection would prejudice the purpose of collection (eg in the case where an enforcement body is investigating a breach of a criminal law).

318. **NPP 1.5** is relevant where it is not reasonable and practicable for the organisation to collect personal information directly from the individual concerned and an organisation collects personal information from a third party. In such circumstances, the organisation must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in sub-clause 1.3. For example, if organisation A collected information from an individual, and organisation A usually discloses that type of information to organisation B, then, at the very minimum, organisation A would be required to tell the individual that it usually discloses the information to organisation B (this is required under NPP 1.3(d)). Before organisation B could collect the information, it would need to be satisfied that the individual was aware of the other matters listed in NPP 1.3 as they pertain to organisation B. If organisation A has given these details to the individual, then organisation B does not have to do any notifying itself. If organisation A has not notified the individual of the matters listed in NPP 1.3 as they relate to organisation B, then organisation B will need to notify the individual of these matters (where relevant) itself. The aim of NPP 1.5 is to ensure that the individual knows what happens to his or her personal information. It does not, however, require organisation B to contact the individual where to do so would pose a threat to the life or health of any individual.

**Principle 2 - use and disclosure**
319. **NPP 2** sets out the general rule that personal information must only be used or disclosed for the primary purpose for which it was collected. Use and disclosure for a purpose other than the primary purpose (a secondary purpose) is only allowed in the circumstances listed in NPP 2. In establishing whether use or disclosure for a secondary purpose is permitted under this principle, it would be appropriate to refer back to the purposes identified under NPP 1.3 or 1.5.

320. Determining the primary purpose of collection should always be possible. Where the information is collected directly from the individual, the context in which the information is provided by the individual to the organisation will be of assistance in establishing the primary purpose of collection. When an individual provides (and an organisation collects) personal information, the individual and the organisation almost always do so for a particular purpose - to buy/sell a particular product or to receive a service, for example. This is the primary purpose of collection, even if the organisation has some additional purposes in mind. Where the information is not collected from the individual, the organisation usually uses the information soon after it collects it and this is a guide to the primary purpose of collection. For example, if an insurance company consults an insurance reference service in the course of considering an applicant, it seems clear that the primary purpose of collection is to decide whether or not to insure the individual.

321. **NPP 2.1(a)** allows information to be used or disclosed for a secondary purpose where the secondary purpose is related to the primary purpose of collection (although where the information is sensitive information it must be directly related to the primary purpose of collection) and the individual would reasonably expect the organisation to use or disclose the information for that secondary purpose. To be “related”, the secondary purpose must be something that arises in the context of the primary purpose. For example, a business that collects personal information about its clients may use that information to notify its clients of its change of business address.

322. Where the information sought to be used or disclosed for a secondary purpose is “sensitive information”, the secondary purpose for use or disclosure must be directly
related to the primary purpose for collection. The sensitivities associated with the use or disclosure of sensitive information mean that a stronger connection should be demonstrated between the primary purpose for collection and the secondary purpose. The application of the “directly related” test in this context is recognised as a matter that can appropriately be clarified in guidelines issued by the Privacy Commissioner.

323. The ‘reasonable expectations’ test would be applied from the point of view of the person in the street, that is, an organisation should be able to use or disclose personal information in ways in which a person with no special knowledge of the industry or activity involved, would expect. For example, if a person has several different types of contact with one bank, he or she could expect the information about themselves to be shared within that bank. If the banking group also ran a health insurance business, the individual would not expect their health claims record to be matched with banking information.

324. NPP 2.1(b) allows information to be used or disclosed for a secondary purpose where the individual has consented to use/disclosure for that secondary purpose. Consent to the use or disclosure may be express or implied. Implied consent would be acceptable in some circumstances. Implied consent could legitimately be inferred from the individual’s failure to object to a proposed use or disclosure (that is, a failure to opt out), provided that the option to opt out was clearly and prominently presented and easy to take up. If the consequences for the individual of the use or disclosure were serious, however, the organisation would have to be able to demonstrate clearly that the individual could have been expected to understand what was going to happen to his or her information. In such circumstances it would generally be more appropriate to seek express consent.

325. NPP 2.1(c) allows personal information (provided it is not sensitive information) to be used for the secondary purpose of direct marketing where it is impracticable to get the individual’s consent before using the information; the organisation gives the individual an opportunity to opt out of further direct marketing communications (at no charge); and the individual has not already asked the organisation not to send direct
marketing material to the individual.

326. This sub-principle allows personal information, other than sensitive information, to be used in order to establish initial contact with an individual, provided that the individual is given the chance to opt out of any further approaches. The exclusion of sensitive information from this sub-principle recognises that the ‘opt out’ mechanism is not a sufficient protection in relation to this type of information. It would allow sensitive information to be used to establish contact with an individual, in the absence of consent, for purposes that may be entirely unrelated to the primary purpose of collection of the sensitive information. The exclusion of sensitive information will not prevent direct marketing organisations from using sensitive information about an individual in reliance on, for example, NPP 2.1(b) (that is, with the individual’s consent) or NPP 2.1(a). The application of this sub-principle in the health context will be detailed in guidelines issued by the Privacy Commissioner.

327. **NPP 2.1(d)** allows an organisation to use or disclose health information for a secondary purpose where the use or disclosure is necessary for research, or the compilation or analysis of statistics relevant to public health or public safety, provided that: it is impracticable for the organisation to obtain the individual’s consent before using or disclosing the information; and the use or disclosure is conducted in accordance with guidelines issued by the Privacy Commissioner under clause 95A; and in the case of disclosure, the organisation reasonably believes that the recipient of the information will not disclose the health information or personal information derived from the health information.

328. In considering whether the use or disclosure of health information is “necessary” the organisation must consider whether the use or disclosure of de-identified information would, in the circumstances, suffice. (This is consistent with the requirement in **NPP 10.4** to take reasonable steps to permanently de-identify health information before disclosing it, where the primary purpose of collection is relevant to research into public health and safety issues etc.) Where the use or disclosure of de-identified information would be sufficient, then organisations must not rely on NPP
2.1(d) to justify the use or disclosure of health information for a purpose other than the primary purpose of collection. In considering whether the use or disclosure is necessary for the compilation or analysis of statistics “relevant” to public health or public safety, “relevant” means that the research is about public health or public safety, or the compilation or analysis of statistics is in relation to public health or public safety.

329. Paragraph 2.1(d)(i) requires it to be impracticable for the organisation to seek the individual’s consent before the use or disclosure. “Impracticability” must be something more than the incurring of some expense or effort in seeking an individual’s consent to the use or disclosure. For example, an organisation may be unable to locate the present whereabouts of the individual for the purpose of seeking their consent, despite making reasonable efforts to contact that individual.

330. Paragraph 2.1(d)(ii) requires the use or disclosure to be conducted in accordance with guidelines approved by the Privacy Commissioner under clause 95A. Clause 95A does not prescribe the content of any guidelines that may be subject to the Privacy Commissioner’s approval. These guidelines may, for example, require different standards to be met, depending on whether the use or disclosure is for the purposes of research or the compilation or analysis of statistics. The guidelines may also require that certain uses and disclosures in reliance on NPP 2.4 be subject to some form of ethics committee approval.

331. If there are no guidelines approved by the Privacy Commissioner for the purpose of this paragraph, this exemption will not operate. An organisation will not be able to rely on this exemption merely because it meets the conditions set out in paragraphs (i) and (iii).

332. Paragraph 2.1(d)(iii) requires an organisation to reasonably believe that the recipient of the health information will not disclose the health information, or personal information derived from the health information. An organisation’s belief that the recipient will not disclose the health information will not be “reasonable” if it is merely assumed.
333. **NPP 2.1(e)** allows information to be used or disclosed for a secondary purpose where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual’s life, health or safety; or a serious threat to public health or safety.

334. The sub-principle is aimed at two types of emergency situations. First, it permits the use or disclosure of personal information where the organisation reasonably believes it is necessary to lessen or prevent a serious and imminent threat to an individual’s life, health or safety. The threat may be to the individual with whom the organisation is dealing, or another individual. The use or disclosure of personal information in response to non-imminent threats to individuals may be dealt with by consent or in reliance on other relevant sub-principles in NPP 2. Secondly, this sub-principle allows use or disclosure where an organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to public health or public safety. There is no requirement that the threat be imminent because a threat to public health or safety, for example, a possible outbreak of infectious disease, may be serious enough to warrant disclosures of personal information but may not be imminent in terms of time. It may be clear that, unless addressed, the threat will do serious harm to public health or safety but unclear when that harm will actually occur.

335. **NPP 2.1(f)** allows information to be used or disclosed for a secondary purpose where the organisation reasonably suspects that unlawful activity has been, is, or may be engaged in, and the organisation uses or discloses the information as part of its investigation into the unlawful activity, or in reporting its concerns to relevant people or authorities. The sub-principle explicitly acknowledges that one of an organisation’s legitimate functions is to investigate, and report on, suspected unlawful activity relating to its operations.

336. **NPP 2.1(g)** allows information to be used or disclosed for a secondary purpose where the use or disclosure is required or authorised by or under law. The sub-principle is intended to cover situations where a law unambiguously requires or authorises the use or disclosure of personal information. There could be situations
where the law requires some actions which, of necessity, involve particular uses or disclosures, but this sort of implied requirement would be conservatively interpreted. The reference to “authorised” encompasses circumstances where the law permits, but does not require, use or disclosure.

337. **NPP 2.1(h)** allows information to be used or disclosed for a secondary purpose where the organisation reasonably believes that the use or disclosure is reasonably necessary to enable an enforcement body (as defined in subsection 6(1)) to perform one of its functions mentioned in paragraphs (i) to (v). This sub-principle recognises that law enforcement includes matters broader than traditional policing of the criminal law, such as confiscation of assets derived from criminal activity, investigation of corruption, serious abuse of power, serious dereliction of duty or other seriously reprehensible behaviour, and breaches of laws imposing a penalty or a sanction. The term “imposing a penalty or a sanction” includes a law allowing the Government to refuse a benefit or impose other non-criminal consequences for failure to comply with a legal obligation, such as a refusal to grant a visa or licence, revocation of a visa or licence or imposing civil penalties under Customs legislation.

338. **Note 1** provides that the NPPs are not intended to deter lawful cooperation with enforcement bodies. **Note 2** makes clear, first, that sub-clause 2.1 does not override any existing legal obligations (for example, the duty of confidentiality between health service provider and patient) not to disclose personal information and, secondly, that an organisation is always entitled not to disclose personal information in the absence of a legal obligation to do so. For example, NPP 2.1(h) would not prevent a medical practitioner refusing to disclose health information to an enforcement body if he or she were concerned about his or her obligation of confidentiality and the body would then need to seek a court order. **Note 3** indicates that any use or disclosure outside Australia must comply with **NPP 9**.

339. **NPP 2.2** requires an organisation to make a written note of the use or disclosure, if it uses or discloses information under paragraph 2.1(h). The requirement to make a note would not apply where there is a specific statutory provision prohibiting the
making of such a record.

340. **NPP 2.3** is a new sub-principle that clarifies the way NPP 2.1 (as it relates to the use of personal information) works where information has been shared between bodies corporate that are related to each other. An organisation that has collected the information from a related body corporate must use that personal information in accordance with NPP 2.1 (or code equivalent). The object of NPP 2.3 is to assist bodies corporate to identify the “primary purpose” of collection so that they are able to establish how they may “use” particular personal information that they have collected from a related body corporate. The sub-principle identifies the “primary purpose” of collection as being the original purpose for which the personal information was provided to/collected by the first point of contact with the group. The fact that the information is shared with other related bodies corporate does not change the “primary purpose” of collection - the purpose is effectively transferred with the information.

341. **NPP 2.4** is intended to permit disclosure of an individual’s health information in a number of circumstances where disclosure would not be permitted under NPP 2.1(e). NPP 2.4 is not intended to operate in a manner that interferes with any existing law governing who may make decisions regarding the health care or medical treatment of a legally incompetent or incapacitated individual. The disclosure of health information under NPP 2.4 to a person who is responsible for an individual does not represent an entitlement for that person to make decisions regarding the health care or medical treatment of the individual.

342. A key limitation on the scope of this sub-principle is that the disclosure can only be made to a person who is responsible for the individual as defined in NPP 2.5. However, a hierarchy does not exist between those categories of person that fall within the definition. That is, the sub-principle permits disclosure to any person listed in NPP 2.5, provided that it is not contrary to any wish expressed by the individual before they became unable to give or communicate consent.

343. An individual may be physically or legally incapable of giving consent because of their mental or psychological state, or their age. An individual may be legally
incapable of giving consent regardless of whether a court or competent tribunal has made a formal determination as to their capacity. Equally, while minors are subject to a presumption of legal incapacity, it is intended that the capacity of a particular minor to give consent be determined on a case by case basis.

344. Another primary limitation on the scope of the sub-principle is that the disclosure can only be made by an organisation that provides a “health service” as defined in Item 17 of the Bill. Paragraphs (a) to (d) set out the conditions that are to be satisfied before an organisation that provides a “health service” can rely on NPP 2.4 to authorise their disclosure of health information.

345. NPP 2.5 lists, for the purposes of sub-clause 2.4, persons that may be taken to be persons responsible for an individual. These include a parent, child or sibling of an individual or spouse or defacto spouse or a relative who is a member of the individual’s household. It also lists guardians, persons exercising an enduring power of attorney for the individual or a person who has an intimate personal relationship with the individual (for example, a girlfriend, boyfriend or partner in a homosexual relationship with the individual). The person may also be a person nominated by the individual to be contacted in case of emergency (for example, on a next of kin card). The terms “child”, “parent”, “relative” and “sibling” are defined in NPP 2.6.

Principle 3 - Data quality

346. NPP 3 provides that an organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date. This principle requires an organisation to take reasonable steps to ensure that personal information is accurate, complete and up to date at the time the organisation collects the information, at the time the organisation uses the information and at the time the organisation discloses the information.

Principle 4 - Data security

347. NPP 4.1 provides that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access,
modification or disclosure. ‘Reasonable steps’ in this context would include following any guidelines prepared by the Privacy Commissioner in relation to limiting physical means of access to personal information, protecting records containing personal information from destruction, physical security measures for safe-keeping of paper and electronic records containing personal information, etc.

348. NPP 4.2 provides that an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. The reference to “needed for any purpose” includes needed for the purpose of meeting a legal requirement to retain the personal information. De-identification requires the removal of any information by which an individual may be identified.

**Principle 5  Openness**

349. NPP 5.1 requires that an organisation prepare a policy statement on its practices relating to the management of personal information. In most circumstances, a general policy statement will suffice stating that it abides by the NPPs or an approved privacy code.

350. NPP 5.2 requires an organisation to provide, to any person who asks, general information about the sort of personal information it holds and how it handles that information. (The obligation to provide a particular individual with access to the information an organisation holds about him or her is covered under NPP 6.)

**Principle 6  Access and correction**

351. As a general rule, an organisation is required to provide an individual with access to personal information held about that individual on request.

352. NPP 6.1 lists the circumstances in which access to the information will be denied. There is an obligation to provide access to personal information, except to the extent that:

(a) other than in the case of health information, it would pose serious and imminent threat to the life or health of any individual;
(b) in respect of health information, it would pose serious threat to the life or health of any individual;

(c) it would have an unreasonable impact upon the privacy of others (that is, an individual should usually be able to gain access to personal information about him or herself but not to personal information about others). Access to a document containing personal information about people other than the individual requesting access need not be denied altogether. In such a case, another person’s personal information may be deleted from the document before the document is released to the individual who made the request;

(d) the request is frivolous or vexatious. An organisation should not be obliged to provide access to personal information where, for example, the individual uses access requests as a means of pursuing some unrelated grievance against the organisation, or makes repeated requests for access to the same information. In order to prevent abuse of this provision, ‘frivolous’ and ‘vexatious’ would be narrowly interpreted - a request for access may be legitimate even if it is irritating to the organisation.

(e) legal dispute resolution proceedings are under way or anticipated and discovery would not grant access to the information. This paragraph does not seek to interfere with the existing procedures for discovery in legal proceedings.

(f) it would prejudicially reveal an organisation’s intentions in relation to negotiations with the individual. An example of this may be where an organisation is currently negotiating with an individual about the purchase of an object and is seeking independent valuations.

(g) providing access would be unlawful. This is intended to cover circumstances where providing access to personal information would ground an action for breach of confidence. This would cover, for example, legal professional privilege.

(h) denying access is required or authorised by or under law (that is, State,
(i) unlawful activity is being investigated, and providing access would be likely to prejudice the investigations into that activity. Organisations have a right and a responsibility to protect themselves against fraud or other unlawful activity. The access principle would not require the organisation to provide access to records which could prejudice such an investigation.

(j) access would prejudice activities being carried on by an enforcement body;

(k) an enforcement body asks an organisation not to provide access because access would be likely to cause damage to the security of Australia. While it is usually preferable that a person be informed of any use or disclosure of their personal information, there will be occasions when that information will itself prejudice an investigation or a security function. The purpose of NPP 6.1(j) and (k) is to ensure that where such information will prejudice an investigation or a security function, then the information will not be passed on.

353. **NPP 6.2** provides that an organisation has no obligation to provide direct access to evaluative information generated within the organisation in connection with a commercially sensitive decision making process. The organisation may, instead, give the individual an explanation for the commercially sensitive decision.

354. **NPP 6.3** is relevant where access would not otherwise be granted (because access is denied under one of the paragraphs in NPP 6.1). Where access would otherwise be denied, NPP 6.3 requires an organisation to consider whether an alternative form of access (through an intermediary) would meet the needs of both parties. The sub-principle is not intended to provide a mechanism to reduce access if access would otherwise be required. There will be some cases - investigations of fraud or theft for example - where no form of access is appropriate. In other cases it should be considered as an alternative to complete denial of access. For example, in the health context, an intermediary could usefully explain the contents of the health record to the individual as an alternative to denying access to the health information altogether.
355. NPP 6.4 provides that charges for access must not be excessive and must not apply to mere lodgement of a request for access. This provision aims to prevent organisations from using excessive charging to discourage individuals from making requests for access. It is reasonable that organisations should be able to charge for providing access to personal information, where complying with a request for access imposes substantial costs on the organisation. In determining what to charge, an organisation should consider reasonable administrative costs ie: the cost of photocopying, for example. An organisation is not entitled to charge an individual for the lodgement of a request for access.

356. NPP 6.5 requires that an organisation take reasonable steps to correct information about an individual where that information is not accurate, up-to-date and complete. ‘Reasonable steps’ has been included so that, if information is shown to be of poor quality but is inaccessible and will never be used, the organisation would not be obliged to expend resources to no purpose. If an individual and the organisation are unable to agree about whether the information is accurate, up-to-date and complete, the organisation must, at the request of the individual, (by virtue of NPP 6.6), take reasonable steps to associate with the information a statement that it is not accurate, up-to-date and complete.

357. NPP 6.7 requires an organisation to provide reasons for denying access or a refusal to correct personal information. The organisation should endeavour to tell the individual which exception under 6.1 it is relying upon to refuse access. However, this would not be required where such a disclosure would prejudice an investigation against fraud or other unlawful activity.

**Principle 7 Identifiers**

358. NPP 7.1 prevents an organisation from adopting an identifier assigned by an agency or a contracted service provider as its own identifier of an individual. For example, it prevents an organisation from acquiring a particular government assigned identifier from all the individuals with which it deals and using that identifier to organise personal information it holds and match it with other personal information
organised by reference to the same identifier.

359. NPP 7.2 provides that an organisation must not use or disclose an identifier assigned by an agency or a contracted service provider unless such use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier to the individual, or in the interests of health or safety or authorised or required by or under law, or in certain other public interests.

360. For example, contracted service providers would be able to use or disclose an identifier if they need to for the performance of a Commonwealth contract. Similarly, organisations that receive funding from an agency could use or disclose the identifier if they need to for performing the functions for which they have received that funding. This principle would not prevent certain organisations from collecting and recording an identifier assigned by an agency for identity verification where authorised under the Financial Transaction Reports Act 1988 (Cth) and Regulation 4 of the Financial Transaction Reports Regulations (that is, the 100 point identity requirements). The purpose of the principle is to prevent the gradual adoption of government identity numbers as de facto universal identity numbers.

361. NPP 7.3 defines ‘identifier’. While not limited to letters and numbers, an identity will often contain either, or both. Examples of identifiers include Medicare numbers and pension numbers.

**Principle 8 Anonymity**

362. Anonymity is an important dimension of privacy. In some circumstances, it will not be practicable to do business anonymously. In others, there will be legal obligations that require identification of the individual. Unless there is a good practical or legal reason to require identification, organisations should give people the option to operate anonymously. This principle is not intended to facilitate illegal activity.

**Principle 9 Transborder data flows**
363. This principle prevents an organisation from disclosing personal information to a recipient located in a foreign country that is not subject to a comparable information privacy scheme (except with the individual’s consent). The principle is based on the restrictions on international transfers of personal information set out in the European Union Directive 95/46. The limited circumstances in which personal information may be transferred to a recipient in a foreign country are listed in paragraphs 9(a) to (f). The principle does not prevent transfers of personal information outside Australia by an organisation to another part of the same organisation, or to the individual concerned.

364. Where personal information is transferred out of Australia by an organisation to another part of the same organisation, clause 5B will apply. Clause 5B provides for the Act to operate extra-territorially in some circumstances.

**Principle 10  Sensitive information**

365. NPP 10 places restrictions on the collection of sensitive information. Sensitive information is defined in section 6(1) to include health information and personal information that also contains information or an opinion about sensitive subjects, such as an individual’s political opinions, religious beliefs or sexual preferences or practices. The collection of health information is specifically dealt with in NPP 10, as it is a subset of sensitive information that involves unique issues.

366. NPP 10.1 describes the circumstances in which sensitive information may be collected. NPP 10.2 and NPP 10.3 set out additional circumstances in which an organisation may collect health information. NPP 10.4 requires an organisation to take reasonable steps to de-identify health information collected in accordance with NPP 10.3, before disclosing it.

367. Under NPP 10.1 an organisation must not collect sensitive information unless: the individual has consented; the collection is required or authorised by or under law; the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual and the individual is physically or legally incapable of
giving their consent or physically cannot communicate consent; the information is collected in the course of the activities of a non-profit organisation; or the collection is necessary for the establishment, exercise or defence of a legal or equitable claim. NPP 10.5 defines “non-profit organisation” as a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

368. Express consent from the individual to collect sensitive information about them would also allow the organisation to obtain consent for all legitimate uses or disclosures of that information. For example, a person who identifies themselves to an organisation as having a particular religious affiliation so that he or she may be treated in a culturally appropriate manner could be asked to consent to the organisation retaining that information for future dealings.

369. An individual who is legally incapable of giving consent to the collection of sensitive information concerning themselves for the purposes of NPP 10.1(c)(i) may be subject to a legal incapacity because of their mental or psychological state, or their age. An individual may be legally incapable of giving consent regardless of whether a court or competent tribunal has made a formal determination as to their capacity. Equally, while minors are subject to a presumption of legal incapacity, it is intended that the capacity of a particular minor to give consent be determined on a case by case basis.

370. In addition to the permitted collection of sensitive information in NPP 10.1, NPP 10.2 sets out a situation in which health information can be collected about an individual. That is, where the information is necessary to provide a health service to the individual and the information is collected as required by law or in accordance with relevant rules dealing with obligations of professional confidentiality.

371. Under NPP 10.3 an organisation may also collect health information about an individual for the purpose of research or the compilation of statistics relevant to public health or safety or for the management, funding or monitoring of a health service provided the safeguards included in NPP 10.3 (b), (c) and (d) are satisfied. These safeguards require that the collection of the health information is the only means to
satisfy the purpose of the research, obtaining the individual’s consent is impracticable and that the information is collected as required by law, in accordance with relevant rules dealing with obligations of professional confidentiality or in accordance with guidelines issued by the Privacy Commissioner. NPP 10.3 recognises the need to enable research to be carried out while at the same time ensuring that appropriate protection is in place for individual’s health information.

372. If health information is collected by an organisation in accordance with NPP 10.3, NPP 10.4, requires the organisation to take reasonable steps to permanently de-identify the information before it is disclosed. For example, if health information is collected to be used in research on a particular disease, the information collected should be modified so that the identities of the subjects of the research are not reasonably apparent in the publication or other disclosure of the results of that research. Information collected pursuant to NPP 10.3 is also subject to the general rules about data security contained in NPP 4.
SCHEDULE 2 - AMENDMENT OF OTHER ACTS

Administrative Decisions (Judicial Review) Act 1977

Item 1. Subsection 3(1) (after paragraph (c) of the definition of enactment)

373. Item 1 inserts a new paragraph (ca) in the definition of “enactment” in section 3(1) of the Act. The addition of new paragraph (ca) means that decisions made by adjudicators under an approved privacy code are decisions made under an enactment and therefore judicially reviewable under the Act.

Item 2. Subsection 3(1) (definition of enactment)

374. Item 2 omits “or (c)” and inserts “(c) or (ca)”.

Customs Act 1901

Item 3. After section 273GAA

375. Item 3 inserts new clause 273GAB into the Customs Act 1901 (“the Customs Act”).

376. New paragraph 273GAB(1)(a) authorises people to give to officers of Customs information (even if the information is personal information) relating to the actual or proposed travel of persons or goods on the way (directly or indirectly) to Australia. Personal information has the same meaning as in the Privacy Act 1988.

377. Similarly, new paragraph 273GAB(1)(b) authorises people to give that type of information to officers of Customs relating to the actual or proposed travel of persons or goods from Australia.

378. The Note to clause 273GAB makes it clear that the Australian Customs Service (“Customs”) is obliged to handle any personal information received in accordance
with section 16 of the *Customs Administration Act* 1985 (which regulates the recording and disclosure of information by Customs) and, more generally, in accordance with the *Privacy Act* 1988. This obligation also applies to the officer who received the information.

379. New sub-clause 273GAB(1) is needed because the National Privacy Principles only authorise the disclosure of personal information for a secondary purpose in certain circumstances (Principle 2.1 refers).

380. The National Privacy Principles allow the disclosure of personal information where that disclosure is required or specially authorised by law (paragraph 2.1(f) refers). New clause 273GAB authorises, in accordance with paragraph 2.1(f), the disclosure of personal information relating to the travel of persons and goods to or from Australia.

381. New paragraph 273GAB(2)(a) provides that section 273GAB does not require anyone to disclose information to an officer. The information intended to be covered by section 273GAB would be given voluntarily to Customs.

382. New paragraph 273GAB(2)(b) provides that section 273GAB does not affect a requirement of or under another provision of the Customs Act for a person to disclose information to an officer. That disclosure can be by answering a question, by providing a document or by other means. There are other provisions in the Customs Act which require people to answer questions or produce documents. Those documents may contain person information. New paragraph 273GAB(2)(b) makes it clear that section 273GAB does not affect those requirements.

*Telecommunications Act 1997*

383. Part 6 of the *Telecommunications Act 1997* sets out arrangements for industry codes and industry standards as part of a predominantly self-regulatory framework for the telecommunications industry. The arrangements involve sections of the
telecommunications industry developing codes and registering them with the Australian Communications Authority (ACA). The ACA has a reserve power to make an industry standard if there are no industry codes or if an industry code is deficient.

384. Paragraph 113(3)(f) of the Telecommunications Act provides that one of the matters that may be dealt with by industry codes and industry standards is privacy and, in particular:

(a) the protection of personal information; and
(b) the intrusive use of telecommunications by carriers or service providers; and
(c) the monitoring or recording of communications; and
(d) calling number display; and
(e) the provision of directory products and services.

Where an industry code deals with a matter set out in paragraph 113(3)(f), the ACA needs to be satisfied that the Privacy Commissioner has been consulted about the development of the code (paragraph 117(1)(j)). Before determining, varying or revoking an industry standard, the ACA must consult the Privacy Commissioner (section 134).

385. The aim of the amendments to Part 6 of the Telecommunications Act is to recognise and promote the pre-eminence of the Privacy Act and the role of the Privacy Commissioner within the telecommunications environment without diminishing the integrity of the current telecommunications self-regulatory regime. The retention of Part 6 of the Telecommunications Act, as modified by the amendments made by this Bill, is necessary for several reasons:

(a) The provisions in Part 6 allow the ACA to request the development of an industry code dealing with privacy. No such power exists for the Privacy Commissioner. With the operation of the default National Privacy Principles (NPPs) it is unlikely that the ACA will exercise such a power but it is useful to retain this power as it is not possible to foresee all eventualities. This power may also provide a useful goad to industry to act under the Privacy Act.
(b) The ACA has also indicated that it believes a number of primarily technical industry codes, which would ordinarily be registered with the ACA, may contain provisions that address one or more of the NPPs, but which do not address all the NPPs. It is important to allow codes which would be more appropriately registered with the ACA to contain provisions which deal with privacy at a very specific, technical level. This is especially important as the Privacy Commissioner cannot register codes unless they address all of the NPPs.

(c) The industry should still be allowed to develop codes which address privacy matters that are not covered by the NPPs and the amended Privacy Act.

**Item 4. At the end of Division 3 of Part 6**

386. Item 4 inserts a new clause 116A into the *Telecommunications Act 1997*. New clause 116A provides that nothing in an industry code registered under Part 6 of that Act or an industry standard determined under Part 6 of that Act replaces or diminishes any obligations imposed by the *Privacy Act 1988* or an approved privacy code as defined in that Act.

**Item 5. Paragraph 117(1)(j)**

387. Item 5 amends paragraph 117(1)(j). Section 117 of the Telecommunications Act provides for the ACA to register certain codes developed by a relevant section of the telecommunications industry. Paragraph 117(1)(j) requires the ACA to be satisfied that the Privacy Commissioner has been consulted about the development of a code relating to privacy and, in particular, the matters specified in paragraph 113(3)(f). The aim of the amendments to paragraph 117(1)(j) is to make it clear that, where the code deals with a matter on privacy and certain privacy matters in particular, as set out in paragraph 113(3)(f), the ACA must be satisfied that the Privacy Commissioner has been consulted about the development of the code by the body or association that represents a section of the telecommunications industry before submitting the code to the ACA for registration.
Item 6.  At the end of subsection 117(1)

388. Item 6 inserts a new paragraph 117(1)(k). Paragraph 117(1)(k) provides that, before registering a code, the ACA must consult the Privacy Commissioner and believe that the Commissioner is satisfied with the code, if the code deals directly or indirectly with the NPPs, or other provisions of the Privacy Act 1988 related to those Principles, or a relevant binding approved privacy code, or provisions of the Privacy Act 1988 related to the approved privacy code.
Item 7.  **At the end of subsection 117(4)**

389. Item 7 inserts a note at the end of subsection 117(4) referring to proposed clause 122A, which will allow the ACA to remove an industry code from the Register. Once removed, the code will cease to be registered.

Item 8.  **At the end of subsection 118(1)**

390. Item 8 inserts a note at the end of subsection 118(1). Section 118 performs the function of being a formal trigger for the development of an industry code. The failure to develop the code which has been requested provides a ground for the ACA to develop an industry standard (section 123). Section 118 provides that if the ACA is satisfied that a body or association represents a particular section of the telecommunications industry, it may request them to develop a code that would apply to participants of the section and deals with one or more specified matters. The note at the end of subsection 118(1) explains that the ACA will be able to request the body or association that represents a section of the telecommunications industry to develop a replacement code for one that the Privacy Commissioner has found to be inconsistent with the National Privacy Principles or a relevant approved privacy code.

Item 9.  **After subsection 118(4)**

391. Item 9 inserts a new sub-clause 118(4A). The sub-clause provides that, before requesting a body or association to make an industry code, the ACA must consult the Privacy Commissioner if the ACA believes the code to be developed may include elements which deal directly or indirectly with the NPPs, or other provisions of the Privacy Act 1988 related to those Principles, or a relevant binding approved privacy code, or provisions of the Privacy Act 1988 related to the approved privacy code.

Item 10.  **At the end of subsection 120(1)**

392. Item 10 amends subsection 120(1). Currently, section 120 provides that changes to an industry code are to be achieved by replacement of the code. Section 120 does not currently allow an industry code to be deregistered. The amendment to subsection
120(1) addresses this shortcoming by providing that if the ACA intends to change an industry code, the ACA is not prevented from removing the code or part of the code from the Register, if it does not wish to replace the code.

393. This amendment is desirable for two main reasons. First, conflicts may arise between privacy codes developed under the amended Privacy Act, or the proposed default regime under that Act, and codes developed under the Telecommunications Act. The proposed amendment enables the ACA to deregister an industry code or part of an industry code that contains provisions setting privacy standards less than equivalent to the NPPs. Second, it is desirable that the ACA should be able to deregister an industry code or part of an industry code for reasons that do not relate to privacy. The ACA should, for example, be able to deregister the whole or part of a code that has become redundant or where the subject matter of the code is more appropriately dealt with by legislation or by a regulator other than the ACA.

**Item 11. After subsection 121(1)**

394. Item 11 inserts new sub-clause 121(1A). The intention underlying Part 6 of the Telecommunications Act is that compliance with industry codes is to be voluntary or as determined by the industry section subject to the code. It is envisaged, however, that where a code is effective and being complied with by a majority of participants to whom it applies, it may be appropriate to direct non-compliant persons to comply with the code. In this context, section 121 allows the ACA to direct the person to comply with a code. This provides a back-up to self-regulation by allowing a person who refuses to comply with otherwise successful self-regulatory arrangements to be directed to comply with a code; in effect, compliance with the code becomes mandatory for that person. New subsection 121(1A) provides that the ACA will be required to consult the Privacy Commissioner before it gives a direction to a person to comply with an industry code that it believes the person has contravened, and the ACA is satisfied that the contravention relates directly or indirectly to the NPPs or an approved privacy code.

**Item 12. At the end of section 122**
395. Item 12 amends section 122 by inserting new sub-clause 122(3). Section 122 currently provides that if an industry participant contravenes an industry code, the ACA may issue a formal warning to the industry participant. This enables the ACA to formally indicate its concerns about a contravention of a code to a person. Such a warning may be a precursor to making a compliance direction under section 121. However, in the case of a serious, flagrant or recurring breach, the ACA may decide to give a direction under section 121 without giving a prior formal warning. Sub-clause 122(3) provides that, before the ACA issues a warning to a person about the contravention of an industry code, the ACA must consult the Privacy Commissioner if the code relates directly or indirectly to a matter dealt with by the NPPs or an approved privacy code.

**Item 13. At the end of Division 4 of Part 6**

396. Item 13 inserts a new clause 122A. Clause 122A will give the ACA a broad power to deregister an industry code or part of a code where the ACA considers it appropriate to do so. If a code is removed from the Register, the code will cease to be registered. If part of a code is removed, the registered code will become the code minus the part. This provision will facilitate alteration of current codes with aspects setting privacy standards less than equivalent to the NPPs. The provision will also give the ACA the power to deregister a code or part of a code for reasons that do not relate to privacy. Possible situations include a redundant code or part of a code, or where the subject matter of the code is more appropriately dealt with by legislation or by a regulator other than the ACA.

**Item 14. At the end of subsection 130(1)**

397. Item 14 inserts a note at the end of subsection 130(1). Section 130 currently allows the ACA to vary an industry standard if it is satisfied that it is necessary or convenient to do so in order to provide appropriate community safeguards or otherwise adequately regulate participants in a particular section of the telecommunications industry. The note explains that the ACA will be able to vary an industry standard that is inconsistent with the NPPs or an approved privacy code,
following advice from the Privacy Commissioner, if the ACA believes it is necessary or convenient to make the variation.

**Item 15. Subsection 134(1)**

398. Item 15 amends subsection 134(1). Section 134 currently provides that if an industry standard deals with privacy issues, the ACA must consult the Privacy Commissioner before determining, varying or revoking the standard. The purpose of the amendments to subsection 134(1) is to clarify that section 134 applies to industry standards that deal with privacy matters and certain matters in particular, as set out in paragraph 113(3)(f), including a matter dealt with by the NPPs, or other provisions of the *Privacy Act 1988* related to those Principles, or a relevant binding approved privacy code, or provisions of the *Privacy Act 1988* related to the approved privacy code.

**Item 16. After subsection 136(1)**

399. Item 16 amends section 136 by inserting a new sub-clause 136(1A). Section 136 currently provides for the establishment and maintenance by the ACA of a Register of industry codes and standards, requests under section 118, notices under section 119 and directions under section 121. Sub-clause 136(1A) provides that the ACA is not required to include in the Register of industry codes and standards a code or part of a code that the ACA removed from the Register under proposed clause 122A dealing with the de-registration of industry codes and provisions of industry codes.

**Item 17. At the end of Division 4 of Part 13**

400. Item 17 inserts a new clause 303A at the end of Division 4 of Part 13. Part 13 of the Telecommunications Act provides for the protection of communications by means of secrecy provisions which create offences for the use or disclosure of certain information by carriers, carriage service providers, emergency call persons and their respective associates. The disclosure or use of protected information is authorised in limited circumstances (for example, disclosure or use for purposes required by or under a law). An authorised recipient of protected information may only disclose or
use the information for an authorised purpose. Division 4 of Part 13 creates offences for secondary or later disclosure or use of information or documents that have been disclosed or used under certain exceptions provided under Division 3 of Part 13. Exceptions to these secondary offences are contained in various provisions of Division 3. The main purpose of the amendments to Part 13 is to ensure its effective operation with the amended Privacy Act and to allow legal proceedings or administrative action to be taken under both the Telecommunications Act and the amended Privacy Act.

401. The effect of clause 303A is that a provision in Division 4 is not to be read down in the light of another provision in that Division or by references in that Division to provisions of Division 3 which also authorise the disclosure of information in specified circumstances.

**Item 18. After Division 4 of Part 13**

402. Item 18 inserts a new Division 4A titled “Relationship with the Privacy Act 1988”. The new Division contains new clauses 303B and 303C.

403. Divisions 2 and 4 of Part 13 currently provide for primary and secondary disclosure/use offences. Section 280 of the Telecommunications Act (in Division 3 of Part 13) provides that Division 2 does not prohibit a disclosure or use of information or document if, amongst other things, the disclosure or use is required or authorised by or under law. Section 297 (in Division 4 of Part 13) prohibits secondary or later disclosure or use of information or documents disclosed as required or authorised by or under law unless the later disclosure or use is required or authorised by or under law.

404. Clause 303B will make it clear that a disclosure or use of information by a person permitted under Divisions 3 and 4 is a disclosure or use authorised by law for the purposes of the *Privacy Act 1988* or an approved privacy code.

405. Sub-clauses 303C(1) and (2) provide that the taking of criminal proceedings under Division 2 or 4 of Part 13 for the unauthorised disclosure or use of information or a document (whatever the outcome of those proceedings) does not preclude civil
proceedings or administrative action being taken in relation to the disclosure or use under the Privacy Act 1988 or an approved privacy code.

406. Sub-clause 303C(3) provides that proposed clause 303C does not affect the operation of section 49 of the Privacy Act. Section 40 of the Privacy Act allows the Privacy Commissioner to investigate certain acts or practices that may be an interference with the privacy of an individual. Section 49 of the Privacy Act provides that an investigation under section 40 is to cease in certain circumstances if certain tax file number or credit reporting offences may have been committed.

**Item 19. Sub-clause 15(2) of Schedule 2**

407. Item 19 amends sub-clause 15(2) of Schedule 2. Part 5 of Schedule 2 provides that a carriage service provider who supplies a standard telephone service must provide itemised billing for each of its customers of such a service. Clause 15 of Schedule 2 allows the ACA to determine that specified details must be shown in an itemised bill provided by a carriage service provider to a customer. In making such a determination, the ACA is required to have regard to the Information Privacy Principles set out in section 14 of the Privacy Act 1988. The amendment to sub-clause 15(2) provides that, in making a determination specifying details that must not be shown in an itemised bill, the ACA must have regard to the NPPs, in addition to the Information Privacy Principles, in the Privacy Act 1988.

*Telecommunications (Consumer Protection and Service Standards) Act 1999*

**Item 20. After subparagraph 147(2)(l)(i)**

408. Item 20 amends subparagraph 147(2)(l) by inserting new sub-subparagraphs (ia) and (ib). Section 147 requires the ACA to make a written determination imposing requirements on telecommunications carriers, carriage service providers and ‘emergency call persons’. In making such a determination, the ACA is required to have regard to the objective that the determination should be consistent with Principle
11 of the Information Privacy Principles (dealing with limits on disclosure of personal
information) set out in section 14 of the Privacy Act 1988 and codes registered, and
standards determined, under Part 6 of the Telecommunications Act 1997 (see
paragraph 147(2)(l)). New sub-subparagraphs 147(2)(l)(ia) and (ib) provide that,
when making a determination on the provision of emergency call services under
section 147, the ACA must have regard to National Privacy Principle 2 (dealing with
use and disclosure) and any relevant binding approved privacy code, in addition to
having regard to Principle 11 of the Information Privacy Principles and
telecommunications industry codes and standards.
SCHEDULE 3 - DISCLOSURE TO INTELLIGENCE BODIES

_Australian Security Intelligence Organisation Act 1979._

**Item 1. Section 93A**

409. Item 1 repeals section 93A of the *Australian Security Intelligence Organisation Act 1979*.

**Item 2. Saving**

410. Item 2 saves the application of section 93A to those acts or practices engaged in before the repeal of section 93A.

_Privacy Act 1988_

**Item 3: After Subsection 7(1)**

411. Item 3 inserts a new sub-clause 7(1A) in section 7. Sub-clause 7(1A) provides for the disclosure of personal information to ASIO and ASIS, without infringing the *Privacy Act*. This item is based on the repealed section 93A of the ASIO Act which exempted disclosures of personal information to ASIO from the Privacy Act in relation to the public sector. This item extends that exemption to disclosures to ASIS and in addition provides that disclosures of personal information to both ASIO and ASIS are exempt in relation to the private sector provisions of the Privacy Act.

**Item 4. Application**

412. Item 4 confirms that acts or practices occurring before and after the commencement of the amendment to section 7 are covered by the amendment.