



ACCI POLICY STATEMENT

PRIVACY POLICY

Privacy has recently emerged as a business issue throughout the developed world. Privacy refers to the handling of personal information. It is also often referred to as 'data protection' which makes it clear that privacy is about personal data, rather than such things as video surveillance, telephone interception, or invasion of physical privacy.

The emergence of data protection as an issue is related to advances in information and communications technologies, which have enabled increased sophistication in the electronic manipulation and use of data. This has seen a heightened consumer awareness of the value of personal information and an expectation of a right to privacy by individuals.

In Australia, federal legislation effective from December 2001 covers the handling of personal information by the private sector.¹ Information held by Commonwealth agencies has been covered by legislation since 1988 and most States and Territories are moving to protect data collected by State and Territory governments.

ACCI advocates a private sector privacy regime for businesses that collect, use, purchase, disclose, or store personal information on individuals based on a light touch regulatory model that provides national consistency, minimal compliance costs for business and certainty for consumers in the private sector's handling of personal information.

PRINCIPLES OF PRIVACY POLICY

A privacy regime for the private sector must:

- be simple and transparent;
- have minimal compliance costs for business;
- give confidence to consumers in the collection, use, handling and storage of personal information by private sector organisations; and
- be outcome oriented with the aim of achieving appropriate protection of information by the most number of relevant businesses.

These principles are reflected in the National Privacy Principles (NPPs) incorporated in the *Privacy Amendment (Private Sector) Act 2000*. They relate to how private sector organisations should handle personal information including how they provide security, access and correction to this information.

Regulation should make a distinction between 'personal information' and 'sensitive information'. Personal information would include information or an opinion that can identify an individual, such as an address. 'Sensitive information', on the other hand, would be information about an individual that can include racial or ethnic origin, religion, health information, financial information, political affiliation, criminal record or sexual preferences. The standards applied to sensitive information would be expected to be more onerous than those applied to personal information generally.

The National Privacy Principles should establish minimum standards that will ensure:

- individuals understand the purpose for which their information is being collected;

- the information is used in ways that are consistent with its collection;
- individuals have the right of access and correction; and
- information about individuals is accurate, up to date, and secure.

The key elements of NPPs should be as follows:

Collection

The collection of personal information must be fair, lawful and not intrusive. A person should be told the organisation's name, the purpose of collection, how that person can get access to their personal information and what happens if the person does not give the information. Where it is reasonable and practical to do so, an organisation should collect personal information directly from the subject of the information.

Sensitive Information

An organisation should not collect sensitive information unless the individual has consented or it is required by law.

Use and Disclosure

An organisation should only use or disclose information about an individual in ways that are consistent with an individual's expectations. An organisation should only use or disclose information about an individual for the purpose it was collected unless the person has consented or the person would reasonably expect such use or disclosure.

Data Quality

An organisation should take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

Data Security

An organisation should take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification, or disclosure. An organisation should take reasonable steps to destroy information if it is no longer needed for any purpose, or permanently de-identify personal information if it is retained for historical or trend purposes.

Openness

An organisation should have a policy document outlining its information handling practices and make this available to anyone who requests this information. An organisation, on request, should take reasonable steps to let individuals know what sort of personal information it holds, for what purposes, and how it collects, stores, uses and discloses that information.

Access and Correction

An organisation should give an individual access to personal information it holds about that individual on request. If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete, and up to date, the organisation should take reasonable steps to correct that information so that it is accurate, complete and up to date. An organisation should provide reasons for denial of access or correction.

Identifiers

An organisation should not adopt, use or disclose, an identifier that has been assigned by an Australian Government 'agency'.

Anonymity

An organisation must give individuals the option to interact anonymously, whenever it is lawful and practical to do so.

Transborder Data Flows

An organisation should only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection that is consistent with the NPPs.

POLICY OBJECTIVES

ACCI believes that the overarching policy objective for a private sector privacy regime is to achieve protection of personal information while still enabling businesses to operate efficiently and effectively.

A successful private sector privacy regime should:

Provide National Consistency and Certainty in Privacy Standards

The provision of nationally consistent privacy standards that will ensure the regulation is 'business neutral' and the same standards will apply for all businesses regardless of location. It will also ensure there is no duplication, conflict or differences in interpretation of regulatory standards between different levels of government.

Be Light Touch and Co-Regulatory

Co-regulation by industry through the development of industry codes should be encouraged because industry codes can be tailored to meet specific industry structures and organisational circumstances and therefore provide flexibility for industry to meet its obligations. Co-regulatory schemes promote good practice and target specific problems within industries, usually impose lower compliance costs on business and should offer quick, low-cost dispute resolution procedures.

Impose Minimal Compliance Costs to Business and Initiate an Effective Awareness and Education Campaign

Every effort should be made to ensure minimal compliance costs to business in the implementation of the private sector privacy regime. The Australian business community should be encouraged as industry sectors and organisations to develop privacy codes and to nominate their own code adjudicator.

Providing education and awareness programs to business is central to maintaining minimal compliance costs and assists business to meet its responsibilities under the Privacy Act in the least intrusive and most cost-effective way. The Office of the Federal Privacy Commissioner should use the existing networks of industry associations in education and awareness programs.

The Office of the Federal Privacy Commissioner should develop fact sheets and simple check lists for business to determine firstly whether they are covered by the legislation and, if so, what steps they need to undertake to comply. The object should be to facilitate compliance by business in the most user friendly and cooperative fashion.

Give Protection and Confidence to Consumers in the Handling, Use and Disclosure of Personal Information by the Private Sector in the Electronic and Conventional Environment

Consumers need to have confidence in the way business deals with the personal information it holds about them. Privacy should not be a major impediment to online purchasing. There should be no distinction between the application of the regime between the electronic and conventional environment.

It should be noted that there are benefits to consumers in the controlled use of the information they have given to a business provided permission has been sought and received from the consumer.

Ensure Efficiency in Privacy Code Approval, Management and Dispute Resolution Procedures

The Office of the Federal Privacy Commissioner should ensure that privacy code approval processes occur expediently and that the ongoing management of privacy codes does not create high compliance costs for business. Dispute resolution processes should be managed efficiently.

ACCI supports a role for the Federal Privacy Commissioner in investigating an act or practice of an organisation that may interfere with an individual's privacy with the aim of reaching settlement through a conciliation process. The Federal Privacy Commissioner in investigations should have regard to the potentially damaging effects of complaints against businesses when carrying out investigations of alleged interferences of an individual's privacy. 'Trial by media' should be avoided.

Maintain Exemptions for Employee Records

The exemption for employee records from the Privacy Act should be maintained. There should be clarity and certainty for employers about the nature of the employee records exemption in the private sector privacy regime. Employers have to be able to take decisions on records regarding the personal and sensitive information of their employees. To the extent that the legislation could be interpreted so as to limit the provision of information to employers to make informed decisions, then it should be amended.

An area of particular concern is health information and the general exemption for employee records. It should be clear how the privacy regime applies to doctors' certificates, medical reports and certificates for workers compensation claims and the results of drug/alcohol testing at work, or by an external doctor or laboratory. As employee records are exempt, then such health information, once it becomes part of an employee record, is not subject to the operation of the Privacy Act.

Have a Small Business Exemption

Small business organisations that do not provide a health service, trade in personal information, or are government contractors, and whose turnover is \$3 million or less, are exempt from the regime. To ensure compliance by those in the small business sector who are not exempt from the regime, government must ensure that there is a simple and effective process of determining turnover and deciding if a small business is covered.

Provide an Opt-In Regime

Businesses involved in cross border exchange of personal information who would not otherwise be covered by a legislative regime may choose to opt in to the legislation framework to meet the requirements of other nations' privacy regimes.

Small businesses not covered by legislation may also choose to opt into the legislation because they believe it makes good business sense or because it may give them a market advantage.

Health Information

The collection, use, storage or disclosure of health information requires special treatment. An organisation should not collect such information unless the individual has consented to its collection or it is required by law.

Health information should encompass information or an opinion about the health or disability of an individual or an individual's expressed wishes about the future provision of health services. A health service includes a wide range of activities:

- assessing, recording, maintaining or improving an individual's health;
- diagnosing an individual's illness;
- treating an individual's illness or disability; and
- dispensing a prescription, drug or medicinal preparation by a pharmacist.

This means that there are many businesses in the health industry that are subject to the Privacy Act, many of which are small businesses. Because protection of health information is likely to be a high profile issue within the community, the compliance needs of the health industry should be addressed by the Federal Privacy Commissioner.

THE POLICY FRAMEWORK

ACCI believes that while personal data should flow freely to enhance trade and commerce, the individual's right to privacy is vital. Unlawful collection, use, storage and disclosure of personal and sensitive information is undesirable.

A co-regulatory approach that allows flexibility of application while providing an effective and comprehensive data protection framework is supported. The privacy concerns of Australian consumers are best addressed if businesses are allowed some room to negotiate appropriate privacy standards with their customers.

An effective multi-faceted education, promotion and general awareness campaign will help meet these challenges.

ACCI encourages the use of existing channels of communication between government and business for the implementation of the private sector regime, including:

- ensuring that industry associations are adequately briefed on the implication of the new regime for their members;
- promoting the economic incentives - that good privacy may mean good business; and
- monitoring whether small businesses have simple and effective means of determining their obligations under the new regime.

ACCI expects that the Office of the Federal Privacy Commissioner will apply the law in a way that encourages compliance and is outcomes based.

Endnote:

¹ The *Privacy Amendment (Private Sector) Act 2000* became effective from 21 December 2001. Australian business has to comply with the provisions covering the collection, use, storage and disclosure of personal and sensitive information. Under the legislation, there are exemptions for small businesses with a turnover of less than \$3 million provided they do not provide a health service or keep health records, trade in personal information, or are a contracted service provider to the Commonwealth. Small business, except for those identified, had until 21 December 2002 to determine whether they were exempt from the legislation. Small businesses opting into the regime were required to comply by 21 December 2002.

For further information:

Greg Evans

Director, Industry Policy and Innovation

Telephone: (02) 6273 3211

Facsimile: (02) 6273 3286

Email: greg.evans@acci.asn.au