

How accountability via government oversight works today in Australia

**Malcolm Crompton, Chris Jefferis and Chris Cowper
Information Integrity Solutions Pty Ltd**

Table of Contents

Introduction	1
Privacy protection in Australia.....	1
Accountability and oversight framework for handling personal information	3
Accountability to the individual.....	5
Accountability to the regulator.....	6
Accountability of the regulator.....	13
Assessing the Privacy Act as an oversight framework.....	16
Assessing the impact of the Privacy Act oversight framework on accountability	18
Conclusion	20

Introduction

The approach to accountability in the Australian privacy law aims to give individuals confidence to participate in the system. In particular it is intended to reassure individuals that when providing personal information they will not face harms such as identify theft, loss of reputation or unwelcome contact.

The law gives organisations legal obligations to protect personal information and to account for their actions. The law also establishes the role of Privacy Commissioner to advise organisations about, and encourage them to meet, their responsibilities to handle personal information appropriately; and to provide redress to individuals if things go wrong.

In effect, the law operates in a multi-layer accountability framework. The law makes organisations directly responsible to individuals and also accountable to the government oversight body, the Privacy Commissioner. The picture is completed by the accountability framework which in turn applies to the Privacy Commissioner.

This paper will start by giving a brief overview of the privacy law and its accountability framework. It will then look at how the framework is working in practice.

The Australian experience is that privacy is best protected where organisations take direct responsibility for meeting their obligations and where the obligations are underpinned by law which includes oversight mechanisms. However, there is always the question of whether the particular mix of law, education, and sanctions currently in place in Australia is the right mix. The paper concludes by looking at what we know so far about whether the oversight framework now in place is making a difference to the protection of privacy in Australia.

Privacy protection in Australia

Development of Australia's privacy law

Australia first adopted privacy law for the handling of personal information during the late 1980s. The *Privacy Act 1988* (Cth) (the Privacy Act) was Australia's response to perceived risks to individuals from increasing use of computers by government department and business. The issues were brought into focus by government proposals to introduce an identity card and to undertake extensive data-matching. The Privacy Act also drew on the guidelines adopted by the Council of the Organisation for Economic Co-operation and Development (OECD) governing the protection of privacy and transborder flows of information.¹

While the Privacy Act initially only applied to the federal public sector it was soon extended to:

- the credit reporting sector, following public controversy over the credit industry's intention to introduce a system of positive credit reporting; and
- data-matching between tax administration and government assistance agencies.²

After that, there was a range of government initiatives in relation to more general privacy protection including the development of a model for self-regulation. However, the Privacy Act did not apply comprehensively to the private sector for another ten years. In 2000, in response to factors including business calls for measures to promote individual confidence in the e-economy,

¹ Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)

² More detail on the history of the Privacy Act can be found on the Privacy Commissioner's website at www.privacy.gov.au and in the Australian Law Reform Commission's Issues Paper 32 Review of Privacy available at www.alrc.gov.au/inquiries/current/privacy/index.htm.

and international developments including the European Union Data Protection Directive, the Privacy Act was extended to apply to much of the private sector.³

While this paper will focus on the Privacy Act it is important to note it only is one of a complex array of laws affecting privacy in Australia.⁴ This means that the oversight arrangements discussed in this paper are not intended to provide a complete picture of the government oversight applying to the handling of personal information by Australian organisations.

Scope of the Privacy Act

The Privacy Act focuses on information or data privacy. It protects personal information relating to individuals where they are directly identified or where their identity can be inferred.⁵ The Privacy Act does not cover other forms of privacy such as bodily privacy, which is the protection of the physical self against invasive procedures or territorial privacy which sets limits on intrusion into a particular area.

The Privacy Act applies to:

- most Federal Government departments and agencies;
- anyone handling tax file numbers;
- the credit reporting sector, including credit providers and credit reporting agencies; and
- much of the private sector.⁶

For convenience, in this paper the term “organisation” will be used when discussing matters that relate to all bodies subject to the Privacy Act unless a more specific term is needed.

Information handling rules

As is the case with data-protection statutes around the world, the core of the protection afforded by the Privacy Act is a set of standards or principles for the handling of personal information. The standards address aspects of the personal information handling process from the point of collection, through storage, use and disclosure.

In line with the fact that the Privacy Act developed over time, and according to different imperatives, it currently contains four similar but separate sets of standards as follows:

- Federal Government departments and agencies must comply with the eleven Information Privacy Principles (IPPs);
- Tax file number recipients (such as employers) must comply with the Privacy Commissioner’s Tax File Number Guidelines covering the collection, use and disclosure of tax file numbers;

³ European Parliament, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/46/EC (1995)

⁴ For more information about the range of Australian laws that may impact on the handling of personal information see Chapter 7 of ALRC Issues Paper 32 noted above.

⁵ See section 6 of the Privacy Act available online at www.privacy.gov.au/act/index.html.

⁶ The Privacy Act exempts small businesses with an annual turnover of \$3 million or less, unless their operation carries privacy risks such as the handling of health information, and certain areas of activity including employee records. For more information see Information Sheet 12 - 2001 Coverage of and Exemptions from the Private Sector Provisions available at www.privacy.gov.au/publications/index.html#

- Credit providers and credit reporting agencies must comply with a range of standards and rules, set out in Part IIIA of the Privacy Act, dealing with collection, use and disclosure of consumer credit information as well as matters such as when a default listing can be made, what information can be listed, and the organisations that may access credit reports;⁷
- Private sector organisations must comply with the National Privacy Principles (the NPPs); the NPPs cover similar ground to the IPPs and in addition have principles for the transfer of personal information across national borders and for anonymity.⁸

The Privacy Act also provides some oversight of, and redress for failure to comply, with standards in two other statutes relating to data-matching and the linking of health data held in relation to separate government funding programs.

Accountability and oversight framework for handling personal information

The Privacy Act builds in organisational accountability by setting information handling standards and giving organisations obligations to protect personal information. To make sure the obligations are met, the Privacy Act also establishes the Office of the Privacy Commissioner, provides that there will be a Privacy Commissioner and gives the Commissioner a defined set of functions and powers.⁹

The Privacy Act also gives individuals the right to complain to the Privacy Commissioner “about an act or practice that may be an interference with the privacy of the individual”.¹⁰ An interference with privacy may arise where organisations’ action are inconsistent with one or more privacy principles.¹¹

Individual complaints are a key focus of action by the Privacy Commissioner where there is accountability failure. However the Commissioner has other functions and powers going to oversight and enforcement. The Commissioner’s direct role in making organisations accountable fits within a wider frame which can be characterised as:

- encouragement (education, advice, guidelines on the application of the privacy principles);
- monitoring (audit, data-matching protocols); and
- enforcement (via individual complaints and some limited financial penalties).

The Privacy Commissioner’s role serves to provide a central point for information about the Privacy Act, for organisations as well as individuals. The Commissioner is also in a unique position to develop a broad overview of how the statute is working in practice as well as undertaking the day-to-day aspects of the role (advice, education, research and monitoring, complaint handling).

⁷ Credit providers and credit reporting agencies that are private sector bodies may also need to comply with the National Privacy Principles.

⁸ In February 1998, following extensive consultation, the Privacy Commissioner issued the National Principles for the Fair Handling of Personal Information as a voluntary guide for business. These principles adapted the IPPs to the private and were later largely incorporated into the Privacy Act as the NPPs.

⁹ See Part IV and sections 27, 28 and 28A of the Privacy Act

¹⁰ See Part V of the Privacy Act

¹¹ See section 13 of the Privacy Act

Nature of principles, the oversight framework and implications for accountability

Before turning to the practical workings of the accountability framework, it is worth noting some features of the privacy principles and the oversight arrangements that are of particular relevance when considering accountability under the Privacy Act.

Firstly, in the main the standards in the Privacy Act are general high level principles rather than a prescriptive list of do's and don'ts. For example, IPP 2, dealing with the notice to be given to individuals before collecting their personal information, requires government agencies and departments "to take such steps (if any) as are, in the circumstances, reasonable...." to give such notice.

As seen in this example, the principles focus on performance of certain duties to protect information without specifying in detail how this may be done. This gives organisations flexibility in how they apply the principles on a day-to-day basis to protect privacy. The principle based approach is often considered to be more adaptable to changes in the regulated environment, for example in business arrangements or technological developments. However, on the downside there is less certainty for organisations as to whether or not a particular practice complies with the principles unless and until there is a complaint.¹²

In turn this may mean that it is more difficult for organisations to know precisely how to effectively discharge their accountability objectives or for individuals to know exactly what to expect. In addition, the question as to whether there has been an accountability failure becomes less a question of testing facts and more a matter of judgement by the Privacy Commissioner. A decision as to whether an organisations' action are consistent with the privacy principles, as well as considering the organisations actions, needs to take into account factors such as:

- the nature of the personal information involved and industry practices;
- the organisation's business circumstances;
- any advice or guidance material available; and
- decisions by the Privacy Commissioner or the courts about similar matters.

However, in contrast to the above, some aspects of the credit reporting provisions are quite specific and prescriptive. Here, the accountability requirements are quite clear. While there will still be a need for education and guidance, if a complaint comes to the Privacy Commissioner, decisions about whether there has been an accountability failure tend to be more factually based.

Secondly, along with a principles-based rather than prescriptive approach to standard setting, the Privacy Act is generally at the lighter end of the enforcement scale. Enforcement of the law comes via a complaint based system with a power to conciliate and to make decisions or determinations (which are then enforceable by the courts) but with power to impose fines limited to some aspects of the credit reporting rules. While the Privacy Commissioner does have monitoring and audit powers in relation to government agencies and department, and the credit reporting sector, these powers do not apply to private sector organisations subject to the NPPs.

Legislative regimes with these characteristics can leave regulators "with substantial uncertainty and ambiguity as they go about implementing and enforcing the law, particularly in the early phases".¹³ This point is considered further later in this paper.

¹² For recent discussions on principles based regulation see *New Governance, Compliance, and Principles-Based Securities Regulation* Cristie Ford University of British Columbia Faculty of Law; Columbia Law School March 11, 2007 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=970130, and *Principles Based Regulation* Julia Black, Professor of Law, London School of Economics and Political Science 28 March 2007 www.econ.usyd.edu.au/claw/seminars/

¹³ 'Light Touch' or 'Soft Touch'? – *Reflections of a Regulator Implementing a New Privacy Regime*, Malcolm Crompton National Institute of Governance, University of Canberra, March 2004 available at www.privacy.gov.au/news/speeches/sp2_04p.pdf

Accountability to the individual

Organisations increasingly need to, or want to, collect personal information about individuals, to administer government programs, complete business transactions or provide services. Historically, the extent to which organisation undertook to be accountable to individuals for the handling of their personal information varied considerably. In some cases, for example where medical or financial information was involved, strong traditions of confidentiality had built up over time. In other cases the interests of individuals in their personal information once it was in the hands of others was given less attention or ignored. Market, social and legal forces all had an impact on how organisations considered and applied accountability concepts.

The privacy principles in the Privacy Act provide an overlay to existing practices, formalising the accountability framework and making it more transparent and detailed. For organisations already working to such arrangements the Act did not mean much change, for other organisations, significant change in practice was required.

Articulating accountability standards and setting them in a legal framework can help the individual know what to expect from organisations in general; although of course first they need to be aware of the law and be able to understand it. The privacy principles work more directly to promote accountability by requiring the provision of information to individuals that will help them assess if the accountability settings are such that they are willing to enter transactions with organisations and then to know if accountability commitments are being fulfilled. For example the principles contain:

- Notice requirements, setting out information to be provided to individuals before personal information is collected, for example about how the personal information is to be used and to whom it might be passed on;¹⁴
- Access and correction rights, giving individuals right to see and correct the personal information organisations hold about them;¹⁵
- Use and disclosure limitations; for example specifying that personal information should only be used for the purpose for which was collected or in accordance with specified exceptions.¹⁶

It is important to remember here that data-protection is one of a number of interests that organisations and individuals have to consider in deciding how to operate or whether to enter into transactions. For example governments will have an interest in resource management and fraud control, business will need to think about profits and costs, individuals may need to receive a government benefit or need to use a service where there are no alternative. So there will be choices for all parties about how to manage personal information and whether it will be provided in the first place. The principles in the Privacy Act help by setting a base line for the handling of personal information and informing individual choices.

While this paper will not consider in detail how organisations are implementing their obligations under the Privacy Act, the steps they have taken include:

- inserting privacy notices on forms and websites;
- developing procedures to provide individuals with access to their personal information;

¹⁴ For example IPP 2, NPP 1.3 and section 18(E)(8)(c) in the Privacy Act

¹⁵ For example IPP 6 and NPP 6 in the Privacy Act

¹⁶ For example IPP 10 and NPP 2 in the Privacy Act

- considering and upgrading physical and information technology security; and
- setting governance processes determining internal access to personal information and permitted uses and disclosures.

Together these measures encourage discipline and transparency in the handling of personal information and help inform individual choices. However, in the Australian context this is not considered to be sufficient to hold organisations accountable for compliance with the Privacy Act; the requirements in the principles are also actionable.

The Privacy Act sets up a framework to allow individuals to take action via complaints to the Privacy Commissioner. The framework is intended to support rather than replace the options that an individual would ordinarily use to resolve a problem. These options range from deciding to not do anything, withdrawing custom or raising their concerns with the organisation and attempting to resolve the matter. In general it is only after this latter step that an individual may ask the Privacy Commissioner to intervene.

Accountability to the regulator

As the earlier discussion has noted, organisations are made accountable to the Privacy Commissioner for their handling of personal information at a number of levels and by a number of mechanisms. The Privacy Commissioner may be collating information to promote transparency, checking if accountability obligations are being met or intervening because things have gone wrong. Organisations therefore may be the respondent to a privacy complaint, called to account for actions in the course of an 'own motion' investigation by the Privacy Commissioner, required to cooperate with an audit process or to provide reports or other information.

While the accountability focus at this level is on organisations and the Privacy Commissioner, individuals are still part of the picture, particularly in the complaint process, but also because it is inherent in the Commissioner's role that the interests of individuals and organisations must both be considered, impartially. Also, as noted above, the right to privacy is neither unlimited nor absolute and the Commissioner needs to consider a range of other issues that may affect an organisation's approach to handling personal information.¹⁷

The discussion so far in this paper has set up the context for consideration of the role of government oversight in achieving organisational accountability for privacy. The key accountability mechanisms in the Privacy Act and how they operate in practice are now set out below. This is not a comprehensive description of the accountability mechanisms but instead focuses on the mechanisms that are currently most in use.

¹⁷ See for example the matters to which the Commissioner must have regard in exercising powers as set out in section 29 of the Privacy Act

Advice and Education

While not directly part of the Commissioner's accountability oversight role, it is worth noting briefly the scope of the Privacy Commissioner's education and advice role. In particular, the Privacy Act gives the Privacy Commissioner functions to:

- provide advice to organisations on any matters relevant to the operation of the Act;
- promote understanding and acceptance of the IPPs, NPPs and privacy generally;
- publish guidelines to assist organisations to avoid interferences with individual's privacy; and
- undertake educational programs to promote the protection of individual privacy.¹⁸

The practical products Privacy Commissioners have used in carrying out these functions include operating a privacy enquiries telephone service, making media releases and announcements, presenting and publishing speeches, conducting training programs and publishing documents and guides as well as convening a privacy contact officers network of officials in government agencies and departments.¹⁹

The Commissioners have also published de-identified case notes of completed investigations to help organisations and individuals understand how the principles in Privacy Act are being applied and how complaints are being resolved.

In practice, in developing information products, guidelines and so on, Commissioners have tended to consult stakeholders, such as organisations and individuals, seeking input and comments. This approach has advantages for the accountability process. The advice produced is more likely to be accurate and relevant to the circumstances in which organisations operate. In addition, the consultation process itself, if well run, will promote understanding of and commitment to the obligations in the Act.

A final point to note that there is some tension in the Privacy Commissioner's role to provide advice to organisations about the application of the privacy principles and the Commissioner's obligation under administrative law to investigate complaints impartially. The challenge for the Commissioner is to provide advice that gives a reasonable degree of certainty while meeting fairness tests and allowing for flexibility and innovation.

Auditing compliance with the privacy principles

The concise Oxford Dictionary defines an audit as "an official inspection of an organisation's accounts".²⁰ In terms of the Privacy Act, the process involves inspecting an organisation's information handling practices and systems to test compliance with privacy principles.

The Privacy Commissioner has functions under the Act to audit compliance by Federal Government agencies with the Information Privacy Principles and with the credit reporting provisions in Part IIIA of the Privacy Act.²¹ It is important to note that the Privacy Act makes the auditing function discretionary. Decisions about how and when to conduct audits, or whether to conduct them at all, are left to the Commissioner. It is also important to note that the

¹⁸ See section 27 of the Privacy Act.

¹⁹ See www.privacy.gov.au for examples of these materials and activities.

²⁰ See the online Concise Oxford Dictionary at www.askoxford.com/concise_oed/audit?view=uk

²¹ Provisions of the Privacy Act relevant to the Commissioner's audit role are: IPPs – section 27(1)(h), tax file numbers – section 28(1)(d) and section 28(1)(e) and credit information files and credit reports held by credit reporting agencies and credit providers – section 28A(1)(g).

Commissioner does not have the power to audit private sector organisation for compliance with the NPPs unless invited to do so by the organisation.

However, where the audit function can be applied, it is a key method for determining the extent of compliance with the Privacy Act. The possibility of an audit also has the potential to encourage organisations subject to the Act to take compliance, and accountability seriously.

The audit process

Privacy Commissioners to date have tended to see the audit process as 'educative' rather than 'punitive' process. The aim is to give organisations an opportunity to understand and respond to privacy risks rather than show up poor practice or to seek to enforce a change in practice.

An audit is by its nature a snapshot of the personal information handling practices relating of an organisation at a particular time and location. The audit process, which begins with the identification of the agency or organisation selected for audit and the proposed audit focus using risk assessment criteria, is basically the same regardless of whether it is an IPP, credit information or tax file number audit.

The usual steps in the audit process, as set out on the Commissioner's website, are as follows:

- notification of proposed audit and request for pre-audit documentation including annual reports, organisation charts, corporate plans, and privacy training approach;
- site visit including inspection of systems, controls and security arrangements and discussion of observations with management;
- preparation of a draft audit report, which outlines the scope of the audit, the systems audited, and the auditors' findings and recommendations;
- provision of draft report to the auditee for comment and response;
- issue final audit report.²²

While as noted above audits have been described and used as an educative tool, there is an enforcement option available. The Privacy Act provides that following an audit the Privacy Commissioner may provide a report to the Minister and the Minister is required to lay a copy of the report "before each House of the Parliament as soon as practicable, and no later than 15 sitting days of that House, after the report is received by the Minister".²³ While to date this provision has not been used, it does provide a strong option where there is a significant issues off concern that that Commissioner is not otherwise able to resolve with a Federal government agency, a member of the credit reporting sector, or a tax file number recipients.

The privacy audit process in practice

The nature of the audit process, involving a detailed examination of an organisations practice, is potentially a rich source of information for the organisation which is audited and other organisations. Privacy Commissioners' annual reports note that audit targets are selected using risk assessment criteria, such as the amount and nature of personal information held, the consequences for individuals if personal information is mishandled and whether a system or program has been in place for a while or only recently introduced.²⁴

²² More information about the privacy audit process, and the Privacy Commissioner's audit manuals are available at www.privacy.gov.au/government/audits/index.html

²³ See section 32 of the Privacy Act

²⁴ The Privacy Commissioner's annual reports from 1997-98 are available online at www.privacy.gov.au/publications/index.html

In practice, the resources available to the Commissioner mean that only a relatively small number of organisations can be audited in any year.²⁵ In some cases an audit will be part of an enforcement activity, for example where a privacy complaint or other source of information suggests there is a systemic failure in information handling practices. However limited number of audits that can be undertaken suggests their impact on promoting accountability will be more in the nature of guidance than enforcement. This has been recognised by Privacy Commissioners, and since July 2002 the finalised reports of audits of Australian and ACT Government agencies have been published on the Commissioner's website.²⁶

While the number of audits per year may be small, analysis of audits over time can provide some insight into how organisations overall are approaching the handling of personal information. For example, in a submission to a Parliamentary committee in 2003 the Privacy Commissioner observed that

generally agencies have a reasonable record in managing the privacy and security of personal information. There are some common audit findings, however, where issues have been identified that indicate more work needs to be done to manage privacy risks and improve practice. In relation to electronic information the common findings include:

- Agencies either do not have adequate IT security policies or such policies are not consistently administered;
- Mass mail outs are an area of particular privacy risk;
- There is a need for greater attention to the security of portable IT devices, such as laptop computers and personal digital assistants (eg. Palm Pilots);
- Agencies may need to more carefully design and test website security measures;
- Agencies need to do more to ensure that their websites display adequate privacy policies, as well as adequate advice to users about security risks.²⁷ Where the agency collects personal information through its site, it needs to ensure there is an adequate IPP 2 (collection) notice; and
- Information technology (IT) outsourcing contracts do not always contain appropriate privacy clauses – and in some cases contracts are not sufficiently monitored.²⁸

Complaints and investigations

Individual complaints are the most direct response to a compliance or accountability failure and are the centerpiece of the Privacy Act's enforcement regime. The Act also provides for:

- representative complaints, where a complaint is made on behalf of a group or class of individuals;
- the Privacy Commissioner to undertake investigations without having first received an individual complaint, known as "own motion" investigations where this seems "desirable"; and
- court injunctions in relation to actions that may be interference with privacy.²⁹

Individuals may complain to the Privacy Commissioner where they think that organisations have mishandled their personal information or, in terms of the Privacy Act, interfered with their privacy. The Act gives the Commissioner the function to investigate complaints and if appropriate to

²⁵ The Privacy Commissioner's annual reports publish information about the number of audits undertaken and a summary of the audit findings. See note 24 above.

²⁶ Published audit reports available at www.privacy.gov.au/government/audits/index.html

²⁷ *Privacy Compliance Audit: Commonwealth Government Websites 2001*, Office of the Federal Privacy Commissioner, available at www.privacy.gov.au/publications/wsr01.html

²⁸ Submission to the Joint Committee of Public Accounts and Audit – Inquiry into Management and Integrity of Electronic Information in the Commonwealth, Malcolm Crompton, Federal Privacy Commissioner, January 2003, section 3.12 pages 12-13 available online at www.privacy.gov.au/publications/wsr01.html

²⁹ The requirements for representative complaints are found at section 38, and the power to undertake "own motion" investigations is found at section 40(2), and provisions relating to injunctions are found at of the Privacy Act,

attempt to resolve the matter by conciliating between the parties.³⁰ The Commissioner is also empowered to decide when to end an investigation; either by a final decision without enforcement powers attached or by a determination, which is then enforceable through the courts.³¹

The Privacy Commissioner has considerable freedom to decide what form investigations take. The Privacy Act sets a few parameters for the handling of privacy complaints, including that the investigation must be conducted “in private” and that before making an adverse determination in relation to a complaint the Privacy Commissioner must give the affected parties the opportunity to appear before him or her and/or to make submissions.³² The Act also gives the Commissioner a range of powers to assist in the conduct of investigations. These powers, which are similar to those provided to other Australian regulators, include the ability to:

- require parties to attend before the Commissioner and produce documents;
- enter and search premises (with consent or a search warrant authorised issued by a Magistrate);
- direct individuals to attend compulsory conferences; and
- take evidence under oath.

The Privacy Commissioner must investigate all legitimate complaints made under the Privacy Act but is given discretion to decline to investigate or to stop an investigation in certain circumstances including where the complainant has not first attempted to resolve the matter directly with the organisation concerned, where the Commissioner decides there is no interference with privacy, or where complaints are vexatious or are more appropriately dealt with by another regulator.

Outline of the complaint investigation process

To assist the parties understand what is involved in the process and, particularly what they can expect from the Privacy Commissioner, the Privacy Commissioner’s Office, provides a range of information on its website.³³ In addition, in 2001, in the context of the extension of the Privacy Act to much of the private sector, the then Commissioner, Malcolm Crompton, published his approach to compliance.³⁴ The approach included, amongst other things, that

The Office will not take action in relation to an organisation without first giving it fair warning of our intentions. Our objective is to assist organisations to comply with their obligations under the Act. Openness and predictability are important means of accomplishing this objective.

The strength of the measures the Office takes in relation to a particular matter will be proportional to its seriousness. The Office will not be taking strong measures in relation to minor breaches of the law. However, in the most serious matters, the Office will be prepared to use any mechanism available under the Act to achieve an acceptable privacy outcome.

In assessing the seriousness of any particular matter the Office will consider:

- the number of individuals involved;
- what disadvantage they have suffered;
- whether the matter raises ongoing systemic issues, or is a one-off incident; and
- the willingness of the organisation to take action to resolve the matter and to prevent recurrence - in assessing this, the organisation’s track record in privacy matters will be taken into account.

³⁰ The National Alternative Dispute Resolution Advisory Council defines conciliation as a process in which the parties to a dispute, with the assistance of a dispute resolution practitioner (the conciliator), identify the issues in dispute, develop options, consider alternatives and endeavour to reach an agreement www.nadrac.gov.au/

³¹ See sections 41 and Division 2 of Part V of the Privacy Act

³² See section 43 of the Privacy Act.

³³ For example see www.privacy.gov.au/privacy_rights/complaints/index.html

³⁴ Information Sheet 13 - The Federal Privacy Commissioner’s Approach to Promoting Compliance with the Privacy Act www.privacy.gov.au/publications/IS13_01.html

The Privacy Commissioner's complaint handling process is essentially a free service; the parties, including the Privacy Commissioner bear their own costs in the process. The investigation process is "inquisitorial" rather than "adversarial" in that the Privacy Commissioner determines the scope of the investigation and decides what information is needed rather than adjudicating on the basis of information that the parties put forward. The Commissioner operates under administrative rather than criminal law and so is not bound by rules of evidence and the decision-making test is "on the balance of probabilities" rather than "beyond reasonable doubt". Generally the parties are not legally represented. However, the Commissioner must comply with the Australian administrative law requirement, including affording "natural justice" to the parties, considering only relevant matters and so on.³⁵

The complaint investigation process, as described on the Commissioner's website, tends to be mostly "on the papers". The Privacy Commissioner puts the individual's allegations, and any evidence to organisations, seeks information and responses and may seek documentary evidence. There are usually no site visits or witness interviews, although these are both possible within the Privacy Commissioner's powers.

The steps in an investigation are usually as follows:

- the Privacy Commissioner receives a written complaint from an individual;
- the complaint is assessed to decide if it falls within the matters the Commissioner can investigate;
- the parties are advised, in writing, that the matter will be investigated and raising initial issues;
- the Commissioner reviews responses and seeks further information or evidence if needed;
- the Commissioner then forms a view about the facts of the matter, and about how the privacy principles apply and puts this view to the parties; and
- the parties have the opportunity to see each others responses, any evidence on which a decision may be based and to provide comments.

An investigation is finalised when the Commissioner is satisfied either that there is no interference with privacy, there was an interference with privacy and it has been adequately dealt with, or the matter is contentious and should be finalised by a formal determination.

The Commissioner is not required to undertake all the steps above. As noted, the Commissioner has the option of attempting to conciliate a resolution to the matters that gave rise to a complaint. Conciliation may be attempted at any stage in the process and if it succeeds the complaint may be closed at that point as being adequately dealt with.

Determinations by the Privacy Commissioner

As noted, the Privacy Act gives the Privacy Commissioner a formal power to make determinations following an investigation of a complaint. The determination power essentially allows the Commissioner to decide on the appropriate remedy for a complaint rather than assisting the parties to resolve the matter between them. The Act provides that the Commissioner's determination may:

- make a declaration that the organisation should not repeat or continue the offending conduct;

³⁵ The Privacy Commissioner's decisions are subject to review under the *Administrative Decisions (Judicial Review) Act 1977*, in a particular section 5 of the Act sets out the requirements for proper decisions-making by administrators, the Act is available online at www.austlii.edu.au/au/legis/cth/consol_act/adra1977396/

- require the performance of any reasonable act or course of conduct to redress the loss or damage suffered by the person concerned; and/or
- require the payment of a specified amount by way of compensation for any loss or damage suffered by the person concerned - loss or damage can include injury to the person's feelings or humiliation suffered by that individual.

The determination power has built in checks and balances. Firstly, as noted above, the Commissioner cannot make a determination that would be adverse to a party without giving the person the opportunity of a hearing before the Commissioner to make submissions orally or in writing. Secondly, if the organisation decides not to comply with a determination, the Commissioner has no direct power to make the organisation comply. Rather, the Privacy Commissioner or the individual concerned may apply to the Federal Court or Federal Magistrates Court to have the determination enforced. The Court then hears the matter afresh and makes a decision which is binding on the organisation.³⁶

The complaints process in practice

The value of the complaint process in the Privacy Act is that it has the potential to provide a relatively accessible low cost remedy for individuals where an organisation has mishandled their personal information. The process also has the potential to influence accountability behaviour in that a privacy complaint to the Privacy Commissioner can have significant consequences for an organisation and so may be something to be avoided. Unless the complaint is clearly outside the Commissioner's jurisdiction or can be dismissed with minimal investigation, participating in an investigation can involve significant costs in staff time, expert advice and so on. If the Commissioner finds an interference with privacy, then there may also be further direct or indirect costs. Typical outcomes following conciliation include:

- apologies
- access provided and/or records amended
- change in practice or procedure
- staff training and
- monetary or other compensation to redress actual loss or damage.

However, it is worth noting that in the nearly twenty year's operation of the Privacy Act, Privacy Commissioners have tended to the conciliation rather than determinative end of the powers available to them. To date Privacy Commissioners have made limited use of the more formal enforcement powers, such as making complaint determinations or seeking injunctions from the court, or publicly 'naming' and 'shaming'. Current Commissioner, Karen Curtis, attributes this in part to:

- the Office's strong focus on conciliation and alternative dispute resolution as a means of resolving individual complaints
- the fact that injunctions are more likely to be relevant in situations where there has been no individual complaint, there is significant and immediate harm and where the respondent is recalcitrant and
- the generally good level of cooperation the Office has received when it pursues issues.³⁷

Privacy Commissioners' use of their coercive powers, and if the powers are sufficient, will be considered briefly later in this paper.

³⁶ To date there has been no actions to enforce a determination under the Privacy Act

³⁷ *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, Karen Curtis, Federal Privacy Commissioner, March 2005, section 5.2 www.privacy.gov.au/act/review/review2005.htm

There are two further observations to make about individual complaints as a means to encourage accountability. Firstly, in order to pursue a complaint, an individual has to be aware of an issue and have sufficient motivation and resources to take it up. While the transparency provision in the Privacy Act should work to assist individuals to take action where things go wrong, it is not clear that they will always, or often, take up this option.

Secondly, the resources applied to an individual complaint may not have the same impact were those same resources applied to an activity that could reach many players, for example, a marketing campaign, a series of targeted audits or an own motion investigation looking an industry wide practice. This is not an easy matter to assess; some recent reflections in the course of reviews of the Privacy Act are mentioned below.

Accountability of the regulator

So far the paper has looked at the role the Privacy Act, as a statutory oversight mechanism, plays in encouraging organisations to take responsibility for protecting personal information. In this context a key feature of the Privacy Act is that it establishes a regulator, the Privacy Commissioner, with a range of powers and functions to: educate; monitor; and enforce. As set out above, the Act can be characterised as a lighter form of regulation. However, it does give the Privacy Commissioner considerable discretion as to how the role is performed, which functions are given priority and which powers are exercised against which organisations.

There are strong advantages in this approach in that the Commissioner is able to respond quickly to changes in the environment or to emerging issues or problems in personal information management. However, with administrative discretion come the potential for abuse of power or mismanagement. In view of this, there are likely to be questions about how the Commissioner in turn is held accountable for the exercise of his or her functions and powers.

In fact, the Commissioner operates within a strong accountability framework. Firstly the Privacy Act, while it gives the Commissioner significant discretion, also sets very clear boundaries within which the Commissioner must operate. Secondly the Commissioner and his or her Office are subject to oversight by the Australian Parliament, bodies such as the Australian National Audit Office and to a range of legal and administrative requirements. The Commissioner also sits within the Australian Administrative law framework, which includes the Commonwealth Ombudsman, freedom of information legislation and judicial review of administrative decisions.

Some of the key accountability measures for the Privacy Commissioner are set out below. The description is not intended to be comprehensive but rather to give a flavour of the arrangements. Before moving to this description, it is first worth making a few comments about how the role of the Privacy Commissioner fits into the Australian government administrative structure. In particular, it is worth noting that the Commissioner has a degree of statutory independence from the Government.

Privacy Commissioner an independent regulator

As set out above, in the context of the Privacy Act, the government oversight role is given to the Privacy Commissioner and his or her Office. In practice, this means that the Office is a separate organisation with control of its own resources, staffing and operating arrangements.

This arrangement is likely to work positively in encouraging organisations to be accountable for their information handling practices. The concentration of the oversight functions in one, separate, Office provides the opportunity to observe and evaluate how they are working. In addition, as a separate body established by statute the Office is given a separate budget allocation which is directed entirely to the oversight role. Again, this facilitates evaluation of the

oversight function, and means that resources do not get diverted to other priorities as might be the case if the role was located in a larger administrative department.

The fact that the Privacy Commissioner is a relatively independent statutory officer is also likely to work positively to facilitate accountability. In Australia, a regulator may have a greater or lesser degree of independence depending on the provisions in its establishing law. A regulator will have a wider scope to act independently and without fear where its governing law has provisions that restrict the conditions under which the regulator can be removed and limit the extent to which external parties can direct its activities.

The Privacy Commissioner has a considerable level of independence, including:

- protection from civil actions and against being sued etc;³⁸
- very limited circumstances when a Minister or the Government can issue a direction to the Commissioner;³⁹ and
- appointment for a fixed term of up to 7 years; strict limitations on when appointment can be terminated; remuneration fixed by an independent external tribunal (without performance pay or other incentives that might be used to attempt to persuade).⁴⁰

In reality the Commissioner operates within a political and social context and does need to communicate and cooperate with stakeholders, including government and business. So, it is important not to overstate the level of independence of the Commissioner. Nevertheless, these characteristics of the role are likely to help set up the expectation that the Commissioner will act impartially and will not be subject to undue influence by government, business or individual interests.

Privacy Act accountability measures

The framework within the Privacy Act builds in a range of measures for ensuring that the Privacy Commissioner is accountable, some of which have been mentioned earlier. In summary these are as follows:

- the role of the Privacy Commissioner is clearly defined in the Privacy Act. The Commissioner cannot take actions that are outside this role without facing legal or administrative challenge⁴¹;
- while the Privacy Act gives the Commissioner considerable discretion, it also sets boundaries and some clear parameters that the Commissioner must follow, for example, as mentioned above, investigations must be conducted “in private”;
- section 97 of the Privacy Act requires the Commissioner to report annually to the Australian Parliament on the operation of the Act; and
- Section 82 of the Privacy Act provides for the establishment of a Privacy Advisory Committee whose role is to “advise the Commissioner on matters relevant to his or her function”.

³⁸ See Part 5 of the Privacy Act

³⁹ For example to report to the Minister on certain investigations, audits etc under section 30,31 and 32 of the Privacy Act

⁴⁰ as set out in Part 4, Division 1 of the Privacy Act

⁴¹ The Commissioner’s functions are set out in sections 27, 28 and 28A of the Privacy Act

External Oversight Bodies

In addition to the accountability measures set out in the Privacy Act, the Privacy Commissioner and the Office are also subject to oversight by a range of government bodies. The two key bodies, whose role and focus are set out below, are the Commonwealth Ombudsman and the Australian National Audit Office.

Commonwealth Ombudsman

The Office is subject to review by the Commonwealth Ombudsman with respect to “a matter of administration”. A matter of administration refers to the way the Commissioner carries out his or her functions rather than the formal exercise of powers under the Act, which are not subject to Ombudsman review. Similarly to the approach in the Privacy Act, review by the Ombudsman is generally triggered by an individual complaint. In other words, if an individual is aggrieved by the way the Commissioner or the Office is dealing with them, has raised the matter with the Commissioner and is not satisfied with the response, then the individual may complain to the Ombudsman. The Ombudsman often will resolve a complaint through a process of conciliation, but when this is not possible, the Ombudsman has the capacity, through a report to the concerned agency, to request remedies, for example, where the action:

- appears to be contrary to law
- was unreasonable, unjust, oppressive or improperly discriminatory
- was in accordance with a rule of law but the rule is unreasonable, unjust, oppressive or improperly discriminatory
- was based either wholly or partly on a mistake of law or of fact
- was otherwise, in all the circumstances, wrong or
- in the course of taking the action, a discretionary power had been exercised for an improper purpose or on irrelevant grounds.⁴²

Australian National Audit Office

The Office is also held accountable for the management of its resources. The annual report mentioned above includes performance management results and financial statements, and is available for oversight by Parliament. In addition, the Office may be subject to an audit by the Australian National Audit Office (ANAO).

The ANAO’s role is to provide the Australian Parliament with an independent assessment of selected areas of public administration, and assurance about public sector financial reporting, administration, and accountability. It does this primarily by conducting performance and financial statement audits.⁴³ ANAO reports are tabled in Parliament and also available to any member of the public.

External Review Rights

Administrative Decisions (Judicial Review) Act 1977

As noted above, complainants and respondents may apply to the Federal Court or the Federal Magistrates Court for a review of ‘administrative decisions’ made about a privacy complaint under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). The ADJR Act provides quite a broad right of review.

However, it is important to note that the ADJR Act reviews the process followed to make the decision, not the substance of the decision. The Court cannot hear the matter afresh or substitute the decision of the Commissioner with its own.

⁴² Information about the role and function of the Commonwealth Ombudsman is available at www.comb.gov.au/

⁴³ See www.anao.gov.au/director/aboutus.cfm

Grounds for a review include a breach of the rules of natural justice, or excess of power, or error of law. If the court finds, for example, that there has been a misuse of power or error of law, the matter will be remitted back to the Commissioner for a reconsideration according to law.

Matters that could be the subject of an ADJR application include:

- a decision that a privacy complaint will not be investigated, or investigated further under section 41(1)(a)-(f) of the Privacy Act;
- a decision not to make a determination under section 52; and
- failure to give to a person who is adversely affected by a decision the reasons for that decision.

Assessing the Privacy Act as an oversight framework

The paper so far has discussed the Privacy Act and its role in the Australian government oversight framework for the handling of personal information and has made some observations about how this is working in practice. It is now worth stepping back and briefly considering how the framework in the Privacy Act measures up against theoretical views on what constitutes “good regulation”.

It is possible to do this from a number of perspectives. A few of the perspectives that have been, or could be, brought to bear on the Privacy Act are set out briefly below.

Former Privacy Commissioner, Malcolm Crompton, took the opportunity to reflect on this question as part of a broader reflection about his time as regulator, when finishing his term of office in 2004. He noted that

“Some regulators have very prescriptive laws, infringement of which can bring heavy criminal penalties. The law may have very extensive powers of investigation, search and seizure, auditing and monitoring. These days, there is a definite trend away from this approach to changing behaviour, especially if it impacts upon businesses. This is partly a response to the difficulty of regulating behaviour in a varied rapidly changing economic and technological environment. Prescriptive law can also lead to a focus on form over substance rather than achievement of the law’s actual objectives. It also reflects a desire to limit red tape applying to businesses.”⁴⁴

The conclusion in the “Reflections of a Regulator” paper was that particularly the private sector provisions of the Privacy Act were “very much a creature of this trend” away from prescriptive regulation. As noted earlier in this paper this less prescriptive style of legislation poses considerable challenges for a regulator. It is also arguable that successful implementation is more dependant on the attributes of the regulator than in a more prescriptive scheme. Malcolm Crompton puts the view that whether or not a regulator is doing the job properly should be considered against tests to establish if the regulation is ethical, effective and efficient. He goes on to mention a number of criteria that might be used to test whether a regulator measures up.

Malcolm Crompton also referred to a discussion on good regulation by Australia’s Productivity Commissioner which put the view that “it [regulation] needs to be *administered by accountable bodies* in a fair and consistent manner”.⁴⁵ As noted above, the Privacy Act framework does include administration by an accountable body suggesting that prima facie it meets one of the tests of this commentator.

⁴⁴ See note 13 above

⁴⁵ *The good, the bad and the ugly: economic perspectives on regulation in Australia* Gary Banks, Chair, Australian Productivity Commission, Conference of Economists October 2003, www.pc.gov.au/speeches/cs20031002/index.html

Another perspective on what constitutes “good regulation” comes from Australian Academics, I Ayres and J Braithwaite.⁴⁶ Ayres and Braithwaite have written extensively on what they refer to as “responsive regulation”. The concept here is that regulators are more likely to succeed if they use strategies and mechanisms that are responsive to the context, conduct and culture of those being regulated, in particular in choosing whether a more or less interventionist response, that is more or less punishment or persuasion, is needed to achieve compliance. Ayres and Braithwaite use the idea of the regulatory pyramid as a way of assessing the right regulatory response in the circumstances. The pyramid organises sanctions or regulatory strategies with the least interventionist, least costly strategies/sanctions at the base of the pyramid and the most interventionist, most costly strategies/sanctions at the top.

The presumption is that regulators should start at the base of the pyramid, and use a persuasive and dialogue based approach to securing compliance—giving the cheaper and more respectful option a chance to work first—and then escalate upwards through the pyramid to invoke the increasing interventionist strategies/sanctions, keeping the more punitive and costly attempts at control in reserve for when persuasion and other lower levels of intervention fail.

Ayres and Braithwaite suggest that if the regulator has strong powers or sanctions available and uses these powers sparingly but when necessary, then this encourages organisations to comply voluntarily with the law, and, if things do go wrong, work cooperatively with the regulator to fix them.⁴⁷

The Australian Law Reform Commission (ALRC), which is currently conducting a review into the Privacy Act, notes that:

In some respects the *Privacy Act* adopts a pyramid-type structure for enforcing compliance. Consistent with the enforcement pyramid model, the approach relies initially on encouraging compliance, with the determinations (and enforcement in the courts) and injunctions held in reserve.⁴⁸

The ALRC, which will be reporting to the Government in March 2008, goes on to seek input on a range of questions in relation to the regulatory structure of the Privacy Act, including:

Is the current compliance model used in the Privacy Act appropriate and effective to achieve the Act’s purposes? If not, is that because of its content, its administration, or some other reason?

Does the range of remedies available to enforce rights and obligations created by the Privacy Act require expansion? For example, should the available remedies include any or all of the following for particular breaches of the Act:

- (a) administrative penalties;
- (b) enforceable undertakings or other coercive orders;
- (c) remedies in the nature of damages;
- (d) infringement notices;
- (e) civil penalties;
- (f) criminal sanctions?⁴⁹

The brief perspectives set out above are not intended to provide a full answer to question as to whether the Privacy Act can be considered “good” regulation. However, the comments above and elsewhere in this paper suggest that the Act has at least some of the elements necessary.

⁴⁶ I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, 1992.

⁴⁷ See note 46 above.

⁴⁸ Australian Law Reform Commission Issues Paper 31 Review of Privacy available online at www.austlii.edu.au/au/other/alrc/publications/issues/31/

⁴⁹ See Question 6.21 ALRC, note 48 above

Assessing the impact of the Privacy Act oversight framework on accountability

The final section of this paper will reflect on the impact government oversight, in form of the Privacy Act, may have on encouraging organisations to be accountable for their handling of personal information and to prevent harm to individuals. It is important to say here that this is a complex question and not one that can be fully answered at this point.

The complexity starts with the fact the Privacy Act is only one of a number of laws that deal with the personal information handling practices of Australian organisations. It is likely to be quite difficult to identify which law may have had a particular effect. Secondly, because the Privacy Act relies on a complaints based enforcement approach, and the Privacy Commissioner has only limited powers to conduct investigations without first receiving a complaint, it is possible that areas of non-compliance could exist without coming to the attention of the regulator. Finally, to date there has not been the kind of detailed qualitative research that would be needed to assess the actual level of business compliance with the Privacy Act.

However, there are a few signposts pointing to an answer. These are:

- Australia’s experience with a self-regulatory privacy protection regime; and
- A recent review of some aspects of the Privacy Act by the Privacy Commissioner.

In addition, as noted in the previous section, the Privacy Act is currently the subject of a review by the ALRC.

Some of the issues relevant to the accountability framework that have been identified or are under consideration in these processes are set out below.

Privacy self-regulation trialed

As noted in a recent speech by Privacy Commissioner, Karen Curtis, Australia trialed a self-regulatory form of privacy protection in the private sector in the late 1990s.⁵⁰ The model was based on a set of privacy principles, the *National Principles for the Fair Handling of Personal Information*, developed by the Privacy Commissioner in consultation with business, government and privacy and consumer representatives. The Commissioner was given a role in assisting organisations to adopt the principles however compliance was voluntary. The scheme was trialed for a short time before other factors, including international developments in privacy protection, led the Government to move to stricter legislation based on law. However, the early experience of the self-regulatory model was that it:

- led to inconsistent standards across industries; and
- did not provide individuals with a clear or easy mechanism to pursue complaints.

Privacy Commissioner’s 2005 review of the private sector provisions of the Privacy Act

As noted above, the Australian Parliament passed law extending the Privacy Act to much of the private sector in 2000. At the time, and in response to issues raised when the law was being considered, the Government committed to review the operation of the provisions. In line with this

⁵⁰ The paper accompanying this speech defines self regulation and provides more detail about the Australian experience – The importance of self-regulation in the implementation of data protection principles: The Australian Private Sector Experience: A speech delivered by Karen Curtis Privacy Commissioner, at the 27th International Conference on Privacy and Personal Data Protection, Montreux, Switzerland, 15 September 2005
www.privacy.gov.au/news/speeches/spdel2005.html

commitment in August 2004 the Attorney-General asked the Privacy Commissioner to undertake such a review. The Commissioner provided her report of the review to the Attorney-General in March 2005.⁵¹ The Privacy Commissioner concluded that there were no “fundamental flaws” in the Privacy Act. However, the Commissioner noted that

The NPPs are based on principles developed in the 1970s and it may be fitting to consider how the operating environment has changed over the last 30 years. For example: Is our definition of personal information still appropriate given technological advances? Do we need different sets of privacy principles covering the private and public sectors? Should the legislation make a distinction between data controllers and data operators? Should the legislation only cover protection of data about living persons? In a changed security environment what are people’s expectations about their personal information?

The Commissioner’s first recommendation to the Government was that it “should consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia”. The Commissioner made 85 other recommendations that covered matters such as:

- the community and business awareness of the Privacy Act;
- impact of the level of resources available to the Commissioner, particular on ability to finalise complaints and pursue an audit program;
- the powers available to the Commissioner;
- the need for a national consistency and a single framework for privacy law.

In the context of the accountability discussion, it is worth noting that a key issue for stakeholders was whether the Commissioner has sufficient powers to effectively implement the Privacy Act. Organisations and business groups generally found that the existing provisions provided appropriate rights and the powers in the Privacy Act were sufficient and they supported the Commissioner’s approach to compliance (as mentioned above this focused on working cooperatively with organisation and making limited use of formal powers). However, consumer and advocacy groups were less convinced. These groups considered both that the Commissioner should use her existing powers more readily and that the Act should have a stronger enforcement regime. The Commissioner did conclude that stronger enforcement powers would be warranted in some areas and that she would consider whether more complaints should be finalised by determination.

Australian Law Reform Commission Review of the Privacy Act

In response the Privacy Commissioner’s report, and a Parliamentary inquiry into similar issues, the Government asked the ALRC to review the Privacy Act.⁵² Interestingly, an ALRC inquiry into privacy in the early 1980s was instrumental in shaping the Privacy Act.⁵³

The terms of reference for the ALRC inquiry asked it to have regard to

:

- the rapid advances in information, communication, storage, surveillance and other relevant technologies;
- possible changing community perceptions of privacy and the extent to which it should be protected by legislation;
- the expansion of State and Territory legislative activity in relevant areas, and emerging areas that may require privacy protection; and
- to consider the extent to which the Privacy Act 1988 and related laws continue to provide an effective framework for the protection of privacy in Australia.

⁵¹ The Privacy Commissioner’s report of her review *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* March 2005 is available online at www.privacy.gov.au/news/alrc_link.html

⁵² Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005)

⁵³ The report of this inquiry *Privacy (ALRC 22)* was tabled in December 1983. and is available online at www.alrc.gov.au/inquiries/title/alrc12&22/index.htm

To date the ALRC has published an issues paper and has undertaken extensive consultation with stakeholders. It is expected to produce a final report in March 2008. A review of the ALRC's issues paper reveals that it is considering in detail many issues that are of relevance to the Privacy Act's statutory oversight role. For example, and carrying through the theme of the Privacy Commissioner's powers, the issues paper has noted that the following options have been raised, in submissions to it, or in other contexts:

- extending the Commissioner's audit powers to the private sector;
- introducing self-auditing and reporting requirements;
- requiring organisations to make available an approved internal dispute resolution process;
- requiring organisations when collecting information to inform individuals of their ability to make a complaint about a privacy issue;
- requiring the preparation of privacy impact assessments in more situations;
- requiring mandatory reporting of privacy breaches.

While the above scan provides only a brief introduction to the issues that have been or are being considered in two significant reviews of the Privacy Act, what it is intended to show is that there appears to be continued support from all stakeholders for a statute based oversight mechanism, and for there to be a regulator. However, the role and powers of the regulator continue to be matters for debate.

Conclusion

Each economy finds its own approach to regulating its particular components. The approach depends on culture, history and other environmental factors. Accountability for the handling of personal information in Australia is just one example.

Indeed, whether a particular accountability regime is effective is similarly affected by environmental factors such as these.

The accountability regime for the protection of personal information in Australia takes a three layered approach at the broadest level: accountability of the organisation to the individual about whom the information relates, accountability of the organisation to the regulator (here the Privacy Commissioner) and third, accountability of the regulator to others including Parliament and its accountability agents such as the Auditor-General and the Ombudsman. Additionally, law in Australia is often subject to periodic review and such a review is under way on its privacy law right now. The end result is a complex of accountability checks and balances.

While always a matter of judgment, there is some evidence that the accountability regime for personal information in Australia is causing organisations to be more responsible in their handling of personal information while always subject to the question of whether it can be improved.