guide edition.01

Privacy Impact Assessments – a guide

August 2004

Office of the
Victorian Privacy
Commissioner

Office of the
Victorian Privacy
Commissioner

Privacy Victoria

Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

GPO Box 5057
Melbourne Victoria 3001
Australia

Telephone +61 3 8619 8719
Local Call 1300 666 444
Facsimile +61 3 8619 8700
Local Fax 1300 666 445

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au

The Privacy Commissioner acknowledges the work of Helen Versey, Deputy Commissioner (Policy & Compliance), Michelle Fisher, OVPC's Manager (Policy), and Andrea Michailidis, Principal Consultant Equal Consulting Group Pty Ltd in the development of this Guide.

TABLE OF CONTENTS

Introduction

Privacy Impact Assessments, known as PIAs, are like the Information Age version of environmental effects statements. PIAs are a practical aspect of balancing new technologies with respect for privacy.

In Victoria's first few years of implementing the *Information Privacy Act 2000*, my office has had experience very similar to other privacy and data protection commissioners around the world. The former New Zealand Privacy Commissioner, Bruce Slane, expressed it with elegant simplicity in the foreword to the New Zealand PIA Handbook –

> *Organisations frequently approach my office asking "Will my project comply with the Privacy Act?"*
>
> *Sometimes this leads to the wider, and perhaps more valuable, questions:*
>
> - *How will my project affect the privacy of individuals?*
> - *Can I achieve my objectives while also protecting privacy?*
>
> *This Handbook provides the tools to help to answer these questions.*
>
> *Protection of privacy is more than simply avoiding a breach of the law. It can involve striving for something better. Privacy impact assessment is one of a range of new techniques which are increasingly being used internationally to better manage privacy risks. Others include privacy compliance audits, privacy seals and associated self-regulatory initiatives and privacy enhancing technologies. Each builds on the bedrock of the enforceable privacy rights for citizens and consumers enshrined in law.*
>
> *Privacy impact assessment enables public and private bodies to make informed choices. It will often be the case that a privacy enhancing solution will be no more difficult or costly to implement that an intrusive one, if the option is identified sufficiently early in project planning.*

I thank my counterparts in New Zealand, Marie Shroff, and Hong Kong, Raymond Tang, for their ready willingness to allow Victoria to model parts of this guide on the work of their offices.

I encourage Victorian public sector organisations to conduct privacy impact assessments, to refine the process and to share their developing knowledge and experience. The technology, the types of information that fuel it, and the ways they are applied in both the public and private sectors, will continually produce variations on the Privacy Impact Assessment.

Feedback from users of this guide is welcome.

PAUL CHADWICK
Victorian Privacy Commissioner
August 2004

What a PIA is

Definition

A Privacy Impact Assessment (PIA) is a systematic process for identifying and addressing privacy issues.[1] It considers the future consequences for privacy of a current or proposed action.

The definition of "impact assessment" provided by the International Association for Impact Assessment is:

"the process of identifying the future consequences of a current or proposed action."[2]

So it is a partly predictive exercise, looking to prevent or to minimise adverse effects on privacy. Typically, PIAs are a series of steps, posing and answering questions and considering options. They can be undertaken during the development of new systems or projects, or when reviewing and perhaps modifying existing systems.

The PIA can be reassurance. It can give confidence to those taking action – and those who will be affected by it – that the impact on privacy has been considered and appropriately addressed. Where legal rights and obligations are affected, this kind of reassurance can be important as a risk management tool and as a way of building trust.

This guide to PIAs is aimed at organisations dealing with the privacy of *personal information* of individuals. It is designed chiefly for organisations working with the Information Privacy Principles (IPPs) in the *Information Privacy Act 2000 (Vic)*.

A PIA may help in identifying issues affecting dimensions of privacy other than information privacy.

The dimensions of privacy are:

- privacy of the body (to protect the integrity of the physical person);
- privacy of the home and belongings (to protect personal space and objects);
- privacy for spoken communications (to protect against eavesdropping);
- privacy for activities that a person undertakes with a reasonable expectation that he/she will not be observed (to protect against surveillance); and
- information privacy (to protect personal information, which may include data about an individual's body, home, belongings, communications and activities).

Respect for privacy upholds the dignity of the individual.

Privacy is precious, but not absolute. PIAs help to get the balance right when several public interests (including privacy) are involved in designing or managing any project or system.

---

[1] PIAs, Blair Stewart, Office of the Privacy Commissioner New Zealand 3 Privacy Law and Report (1996) 61.

[2] http://ww.iaia.org/

When to do a PIA

When considering whether to do a PIA, the first thing to ask is whether the information you are dealing with is "personal information" within the meaning of section 3 of the *Information Privacy Act.* [3] A PIA should be completed for any new project or system, or any significant revision or extension of an existing system, involving the collection and handling of personal information.

Some examples of activities that are likely to benefit from a PIA are:

- existing, new or increased collection, use or disclosure of personal information;
- creation or modification of databases dealing with personal information;
- merging of internal databases;
- introduction of new information technologies;
- adoption of identification and authentication methods (especially biometrics[4]);
- data matching or aggregating personal information within the organisation;
- linking of databases within the Victorian Public Sector or between the Victorian Public Sector and private sector entities;
- transfer of personal information outside of Victoria both one-way or as an exchange, including with federal, state or territory public sector entities or the private sector, and including transfers overseas; and
- creation of a new public register or renovation of an existing public register.

Having decided to do a PIA, consider its timing. Ideally, a PIA should be initiated at the early stages of project or system development and planning. Your early consideration of privacy issues through the PIA will be a factor in the assessment of resources needed for a project and should prevent unnecessary effort being expended on options incompatible with the IPPs. Often, a PIA will be useful more than once in the project's life. The PIA should be dynamic, updated as changes are contemplated to projects. It should be revisited at various times throughout the system or project development. The PIA will then form an integral part of project management and decision-making processes. In this sense, PIAs are a practical tool for making data protection part of an organisation's culture, so that in time it becomes more automatic, more reflex.

The evolving nature of the PIA means it may become a more detailed document over time with the continued development of a particular project or system. Importantly, the PIA can be used to monitor changes with potentially negative implications for the privacy of individuals[5].

---

[3] See the Victorian Privacy Commissioner's *Guidelines to the Information Privacy Principles: Part One* pp 6-7 for guidance on identifying personal information within the meaning of the *Information Privacy Act.*

[4] Biometrics are the use of an individual's unique physiological or behavioural characteristics in identifying or authenticating the individual. Biometrics include, but are not limited to, a person's fingerprint, face, gait, iris or signature.

[5] David H Flaherty, Ph.D Professor Emeritus, University of Western Ontario "Privacy Impact Assessments: An essential tool for data protection" p 11. A presentation to a plenary session on "New Technologies,

Why is it useful to do a PIA?

Value to organisations

A Privacy Impact Assessment is often described as an "early warning system" for your organisation. It allows you to detect potential privacy problems, take precautions and build tailored safeguards before – not after – you make heavy investments in time and perhaps in technologies. PIAs help identify inherent privacy issues that may be costly to address later in the project.

The PIA affirms that privacy issues have been addressed and that reasonable steps have been taken to provide an adequate level of privacy protection at the time of assessment. The PIA also provides a mechanism for reviewing the privacy impact of proposals as changes occur.

The object of a PIA is not to "sell" an idea that may have adverse privacy implications. The primary object of a PIA is to allow any adverse effect on privacy to be weighed properly against whatever benefits the project or system offers in the public interest. The *Information Privacy Act* aims at a balance, in particular circumstances, between the public interest in the free flow of information and the public interest in privacy. That said, a by-product of a good PIA may well be that it helps reassure people that a trade-off of privacy is worth it, or that promised safeguards can work.

A PIA can benefit an organisation because it:

- helps identify the effects a project, initiative, proposal or system might have on individuals' privacy;
- assists in anticipating the public's possible privacy concerns;
- helps to ensure compliance with the Information Privacy Principles;
- promotes awareness and understanding of privacy issues inside the organisation;
- helps reduce cost later in management time, legal expenses and potential media or public concern by considering privacy issues early;
- enhances informed decision-making at the right level; and
- enhances the legitimacy of a system or proposal, especially where some compromise or trade-off is necessary.

PIAs – your approach to IPP compliance

The Privacy Impact Assessment will provide assurance that the 10 Information Privacy Principles in the *Information Privacy Act* are taken into account at all stages of the development of a project, program or service. The Information Privacy Principles are the key to complying with *Information Privacy Act*.

Security and Freedom," at the 22nd Annual Meeting of Privacy & Data Protection Officials, Venice, 27-30 September 2000.

The complete text of the IPPs forms Resource 3 of this guide.

Summary of the IPPs

This is a short summary of the IPPs:

IPP 1 Collection. Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to personal information.

IPP 2 Use and disclosure. Use and disclose personal information for the primary purpose for which it was collected, or in accordance with any of eight categories of use and disclosure found in IPP 2. These categories include: related secondary purposes; consent; public safety; research; purposes authorised under other law; and crime and misconduct investigations.

IPP 3 Data quality. Take reasonable steps to keep personal information accurate, complete and up to date.

IPP 4 Data security. Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.

IPP 5 Openness. Document clearly expressed policies on management of personal information and provide the policies to anyone who asks.

IPP 6 Access and correction. Individuals have a right to seek access to their personal information and make corrections. Access and correction will be handled mostly under the Victorian *Freedom of Information Act*.

IPP 7 Unique identifiers. A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisation's operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP 7 limits the adoption and sharing of unique identifiers.

IPP 8 Anonymity. Give individuals the option of not identifying themselves when entering transactions with organisations, if that would be lawful and feasible.

IPP 9 Transborder data flows. If personal information travels, privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs.

IPP 10 Sensitive information. The law restricts collection of sensitive information like an individual's racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.

Guidelines are available at www.privacy.vic.gov.au >Publications >General Information >Guidelines.

How, in practice, could a PIA bring these IPPs into better focus for the planners of a project? Examples follow.

Example 1 – IPP 1 Collection

Information Privacy Principle 1 states that an organisation should collect only personal information that is necessary for performance of functions.

The Privacy Impact Assessment will:

- highlight whether your organisation has personal information and if it does what you are going to do with the personal information in relation to this project;
- assist you to examine the way personal information is handled throughout your organisation and decide whether you really need to collect personal information as part of the project or can you proceed without it. If you decide you need the personal information, the PIA will focus on whether that information can be de-identified, yet still fulfil your project's objectives; and
- highlight whether your authority to collect the information has been established. This could be a legal authority or authority obtained through an individual's agreement.

Thinking about these issues through the PIA process will not only minimise collection of unnecessary personal information, but it can also reduce operating and systems costs.

Example 2 – IPP 3 Data quality

Information Privacy Principle 3 states that an organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

The Privacy Impact Assessment will:

- identify if your information system permits information to be corrected;
- identify if your information system keeps records of when data was last up-dated or modified; and
- get your systems designers thinking early about how to ensure data quality, which will improve decisions made later on the basis of that data.

Example 3 – IPP 4 Data security

Information Privacy Principle 4 says that an organisation should take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.

The Privacy Impact Assessment will:

- identify what areas are at risk and what security arrangements are needed; and
- help you assess whether the personal information is protected by security procedures commensurate with the sensitivity of the information.

Example 4 – IPP 5 Openness

Information Privacy Principle 5 requires organisations to have clearly expressed policies available to anyone who asks for them.

The Privacy Impact Assessment will:

- highlight what your policy should cover including what the organisation does with the personal information, what it needs to do, what it properly can do and how it complies with what the organisation says it is doing; and
- identify how the policy will be made available, for example through publishing the policy in full, or in condensed versions that suit the project's needs and context. (See, for example, Website Privacy Guidelines at www.privacy.vic.gov.au >Publications >General Information >Guidelines.)

Example 5 – IPP 9 Transborder data flows

Under Information Privacy Principle 9 an organisation needs to ensure that if personal information travels, privacy protection travels with it.

The Privacy Impact Assessment will:

- show in advance which information will leave Victoria and where it will go. In some cases, the handling of IT and data collection/storage by a contracted service provider will be envisaged by the project's planner. It may be that the relevant servers are physically located in another state or overseas. The same may be true of the data processing/key boarding/or call centre aspects of a project. IPP 9 needs to be considered. The project's contractors and sub-contractors can usually deal with the requirements of IPP 9 (or NPP 9 under the Commonwealth *Privacy Act* for the service provider in some contexts). The point here is that the PIA will identify those issues early and allow you to deal with them in an orderly way; and
- help you determine the steps necessary to protect the personal information as it flows across borders eg. does the contract cover it? Is the recipient covered by data protection law similar to the Victorian *Information Privacy Act*?

Once you have been through the PIA process in relation to each IPP, you will be able to assess the privacy risks associated with your project. You can then determine whether the risks are avoidable, what options you have and what cost effective steps can reduce them to an appropriate level. The final decisions about where the balance lies will be for the appropriately senior decision-makers. But the first steps are to diagnose for them what the risks, benefits, costs and safeguards are – this is primarily what a good PIA will do.

Implementing the PIA process in your organisation will demonstrate to employees and contractors that data protection is taken seriously and that it needs to be thought about into the future.

Value to the public

A proper PIA can give the general public confidence that their privacy has been adequately considered and addressed. Demonstrating that your organisation has identified and managed privacy issues in a particular project builds and sustains trust with the public and other agencies. If you demonstrate that you take privacy seriously, you are demonstrating respect for people. People who are confident that they and their privacy are respected are more likely to provide the information and co-operation that will make your projects and systems successful. The PIA should be seen as a source of information and action to allay fears about loss of privacy or about protection of personal information. It can also assist in anticipating public reaction to the privacy implications of a given proposal.

Releasing PIAs gives the public an opportunity to express concerns and have them addressed before a project has been implemented. One of the primary objects of the PIA is to increase transparency in the handling of personal information by the public sector (*Information Privacy Act*, s 5).

A number of the IPPs require that an organisation take reasonable steps to meet a certain standard. The PIA process and the public release of the PIA can be reasonable steps in several contexts. The fact of having done a PIA itself may assist in demonstrating compliance in the context of a subsequent complaint, privacy audit or compliance investigation. Imagine that your organisation suffers a security breach and personal data goes missing or turns up in the wrong hands with harmful consequences. If individuals complain under the *Information Privacy Act*, IPP 4 (data security) will likely come into play. Of course, the facts in each case will be central, but it is likely that an organisation will be in a better position if it can show it considered in advance its data security risks and analysed the potential for unauthorised disclosure or misuse. Although the protections may have failed in the particular instance, the PIA will be evidence of advance consideration of data security and other privacy issues.

Consider another example. IPP 1 states that an organisation collecting personal information must take reasonable steps to ensure that the individual is aware of –

(a) the identity of the organisation and how to contact it; and
(b) the fact that he or she is able to gain access to the information; and
(c) the purposes for which the information is collected; and
(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and
(e) any law that requires the particular information to be collected; and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

Under IPP 5 (openness), an organisation must take reasonable steps to let the person know generally what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information. The PIA can be one means of demonstrating that the reasonable steps required in the IPPs have been anticipated, planned and, in many respects, undertaken.

Who should do a PIA?

Choosing the right people

The PIA will be of value to project managers, information technology specialists, policy makers, legal advisers, human resource advisers and privacy officers involved in the particular project or system.

The skills required to undertake a PIA will vary depending on the proposal being evaluated but, in general, analytical and writing skills will be required. A Privacy Impact Assessment can be performed by:

- an individual from within the organisation;
- a team or section from within the organisation;
- joint team or working group if more than one organisation is involved in a project; or
- an external body.

The "Privacy Impact Assessor", whether an individual or a group, needs to be familiar with the Information Privacy Principles and be able to help others understand them. Finding the right people with the right skills will make the PIA process easier and quicker.

Using the organisation's own resources and personnel to conduct the PIA gives the organisation a sense of ownership of the PIA. It uses and builds experience and internal expertise to identify privacy issues and to handle later what the PIA process identifies or anticipates.

The nature and size of the proposal, project or system may determine whether an internal individual or team conducts the PIA, with or without external specialist advice. By-products of doing a PIA internally are the way it grows and reinforces the organisation's knowledge base about privacy and data protection, and (depending on the seniority of the leader) the way it signals to the organisation's staff the significance that senior management attaches to getting privacy right.

Where the PIA is undertaken by staff rather than a specialist external consultant, you may wish to consider incorporating external opinion on the result before finalising the PIA. Outsiders often ask useful questions that insiders have not considered because of their familiarity or assumptions. Some external involvement may be useful in building public confidence in the PIA later.

External consultants with particular skills may also be brought in to assist only with certain aspects. In either case it will still be important for the organisation to have overall responsibility for the PIA.

How to focus a PIA

Project management methodologies

Robust project management methodologies include planning and business case phases, incorporating consideration of the regulatory environment. In a sense, PIAs form part of the risk evaluation and management tasks for any substantial undertaking.[6]

Information's life cycle

The PIA focuses on the life cycle of personal information. It should describe:

- the type of personal information collected;
- the original source of the information;
- the circumstances for collection;
- the processing of that information;
- the intended use of the information;
- who the information will be distributed to;
- the circumstances in which processing, use and disclosure take place; and
- the safeguards that will operate against misuse, loss, unauthorised access, modification or disclosure.[7]

Focussing on the life cycle of the information will help you determine at which points information decisions are made and where privacy becomes particularly vulnerable.

Data flow diagrams

Diagrams depicting the flow of personal information can be valuable in the PIA process to show clearly, for instance: how data is collected; how it circulates internally; and where it is disseminated beyond the organisation.

Key areas

In a broader context the PIA will require analysis in the following key organisational areas:[8]

---

[6] Some prominent project management methodologies are either prescribed or strongly recommended in the VPS. These are:

- Gateway Review Process. Details are available at www.dtf.vic.gov.au
- PRINCE2 . Details are available at www.ogc.gov.uk/prince
- Project Management Body of Knowledge (PMBOK). . Details are available at www.projectsmart.co.uk/pmbok.html

[7] *Privacy Impact Assessment: Some Approaches, Issues and Examples* Blair Stewart e-Privacy in the New Economy Conference Paper, March 2001 p 4.

People

People are the key to privacy protections and, usually, to breach. Focus on conveying to people an understanding of why privacy matters. This is a foundation for consistent compliance. Consider how to use training, organisational awareness, manuals and other forms of guidance and communication of privacy policies.

Process

Type of personal information collected, why and how it is collected, how privacy is assured operationally and what mechanisms provide individual access to information. This includes:

- establishing procedures to log, review and resolve complaints about breaches of privacy; and
- establishing a system for reviewing existing processes.

Physical environment

Physical space where personal information is stored, physical security measures and the availability of secure document disposal facilities.

Technology

System design characteristics, data security and integrity measures and access controls.

Accountability

Who will be responsible for compliance with privacy requirements, who will decide whether a PIA is required, and who will manage the PIA.

Risk assessment

Risk assessment involves discussion of collection, use, disclosure and retention of personal information.

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or disclosing sensitive details more widely than justified, all involve risks both to individuals' privacy and to the organisation's compliance and reputation. Risk assessment sorts out which risks are serious and which are trivial.[9]

---

[8] Ontario Information and Privacy Office *Privacy Impact Assessment: A User's Guide* at: http://www.gov.on.ca/MBS/english/fip/pia/pianew.html p 25.

[9] Office of the Privacy Commissioner New Zealand. *Privacy Impact Assessment Handbook* at: http://www.privacy.org/comply/pia.html

Formulating the right questions

The art of an effective Privacy Impact Assessment is to ask the right questions. This will provide the information needed to make the proper assessments.

Resource 1 of this guide includes a list of generic questions designed to apply to any project. They are a guide only. Each project will be different. More focussed questions may be needed to address particular issues in particular contexts.

Doing the right follow-up

Once the Privacy Impact Assessment is complete, the privacy issues identified may need addressing to ensure the project complies in the most efficient and confidence-building way. For example you may need to:

- seek legislative change to your own Act. For example, for some new project you may be proposing to use or disclose personal information already collected for unrelated, different purposes, and you may need to get the new use/disclosure properly authorised by an express amendment;
- (short of legislative change), clarify that the appropriate decision-makers have given clear authority for what is envisaged and that they have the requisite power under law to do so;
- make changes to existing organisational processes and systems. For example staff may need to be retrained, information systems modified or different accountability measures introduced; and
- develop a Part 4 *Information Privacy Act* Code of Practice. A Code gives an organisation which handles personal information flexibility in the way that they manage that personal information by setting standards that differ from the IPPs – as long as they are at least as stringent as those prescribed by the IPPs. A good PIA should make the Code-making process easier.

Once the PIA is complete, some privacy risks of the project are likely to continue and consideration needs to be given to how these will be managed. In particular you will need to determine who will be accountable for future privacy management of the project after the project's set-up team moves on and the operation perhaps becomes "routine".

This is especially important if the project was developed by consultants, who will leave with their knowledge unless the project requires clear hand-over arrangements. Consideration also needs to be given as to how changes that occur during the life of the project will be handled, such as when and how will the PIA be updated and reviewed.

Making your PIA public

There are two aspects to making your PIA public – *public consultation* as part of a PIA and *publishing* a PIA once it is complete.

Public consultation not only addresses the question of independent scrutiny, but also generates confidence amongst the public that their privacy has been considered. Matters that may influence your decision to undertake a wider consultation might include:

- whether there is likely to be public concern about actual or perceived impact on privacy;
- whether there is a large number of people whose privacy is affected, or a particularly vulnerable group;
- whether your initial thinking indicates that new formal authority will need to be obtained for the collection and handling of personal information that the project envisages. If so, then the method of authorisation will be relevant to the issue of public consultation. If legislative change is needed, a Cabinet and Parliamentary process will necessarily involve public announcements and debate. If a Part 4 *Information Privacy Act* Code is to be sought, that process also provides for public consultation. So the project's own needs may affect decisions about the method and timing of making the matter public. The PIA itself may not be the proper vehicle for public consultation every time. Transparency may come at a later stage than the PIA itself, but the contents of the PIA will very often assist the subsequent consultation;
- whether there is already a formal consultation process into which the privacy aspects can be incorporated; and
- the need to build trust in a new practice or a new technology.

The *Information Privacy Act* emphasises the 'transparent' handling of personal information.[10] In the PIA context, that indicates public consultation. But, in particular projects, security may be a consideration. A good, thorough PIA may necessarily analyse the data security weaknesses of a project in order that they can be minimised. To make the analysis public may undercut the precautions taken and the ultimate aim – better data security. In such cases, a properly edited PIA will usually suffice to balance the security and transparency interests.

[10] Section 5.

Resource 1: the right questions

These questions are intended to be useful in a variety of settings. They are by their nature generic. Not every question may be relevant to your proposal. Your proposal may need a more detailed or specifically focussed privacy impact assessment. These questions are designed to initiate your thinking about common issues that arise and impact on privacy.

Before you begin – do you need to comply with privacy laws?

"Personal information"	Does the *Information Privacy Act* apply? Does the proposal involve the collection or handling of "personal information" – ie. information about a person whose identity is apparent or can reasonably be ascertained? Or can you use information that does not identify a person or is anonymous?
Exemptions	Do any of the exemptions in the *Information Privacy Act* apply, namely:
(i) courts or tribunals	Is information being collected or handled by a court or tribunal in the exercise of judicial or quasi-judicial functions?
(ii) generally available publications	Is information being used from a generally available publication (not being a public register, to which some privacy obligations continue to adhere)?
(iii) law enforcement agencies	Is the information being collected or handled by a law enforcement agency? If so, a limited and conditional exemption may be available. The exemption applies where non-compliance is reasonably necessary, and the exemption does not apply to all the IPPs.
Health information	Does the proposal involve the collection or handling of health information? If so, then the Victorian *Health Records Act 2001* (or Commonwealth *Privacy Act 1988*) may apply.
Surveillance devices	Does the proposal involve the use of surveillance devices (such as cameras or location tracking devices)? If so, then the Victorian *Surveillance Devices Act 1999* may apply.
Common law or statutory duties of confidence or secrecy	Is the information you intend to collect or handle subject to any common law or statutory duties of confidence or secrecy? Are these obligations inconsistent with (and therefore prevail over) the *Information Privacy Act*, and to what extent?

Transborder data flow and private contractors (IPPs 9; s 17)

Participants from the private sector or from outside Victoria	Who else is participating in the collection, disclosure and handling of the personal information? Are participants from the private sector or from a jurisdiction outside of Victoria? Do other privacy laws or privacy protective regimes (eg, administrative privacy standards) apply? How do these compare with the *Information Privacy Act* and IPPs?
Cross-border data sharing	Where information is to be transferred outside Victoria, is the recipient organisation bound by a privacy law or binding scheme that is substantially similar to the *Information Privacy Act*? Is it necessary and practicable to seek consent to the transfer? What steps have been taken to ensure that the information will be handled in the other jurisdiction in a manner that is consistent with the IPPs?
Contracted service providers	Will the information be collected or handled by a contracted service provider? Are the activities under the contract exempt from the Commonwealth *Privacy Act*? Is the contracted service provider bound by the contract or otherwise (eg. by a code of practice) to comply with the IPPs or some other privacy standard?

Collection (IPPs 1, 8 and 10)

Clear and legitimate purposes	Why is the information being collected – for what purpose/s? What public interest/s justify the collection? Have the purposes been clearly specified?
Necessity	Is it necessary for the organisation to collect the information? What evidence is there to support the need for the information?
Proportionality / intrusiveness	Is it necessary to collect the information in the manner, and to the extent that is proposed? Are there other alternatives available that will be less intrusive?
Effectiveness	Will the collection be effective in achieving the legitimate purpose justifying collection? How, and when, will effectiveness be assessed / reviewed?
Lawful authority	Does the organisation have lawful authority to collect? Where the organisation is established by statute, does the statute expressly or impliedly authorise the proposed collection and handling of information? Does an Act require amendment to provide the necessary lawful authority, or to revise a statutory prohibition?

Anonymity	Who is the information about? To what extent can anonymity/pseudonymity be preserved? Where personal identifiers are not used or have been removed, how readily can a person be re-identified?
Sensitive or delicate information	What information is being collected? Does the collection include sensitive, intimate or delicate information? Additional care may be necessary for intimate or delicate information (through, eg, a tailored Code of Practice). Sensitive information can only be collected if one of the conditions in IPP 10 is satisfied (eg, with consent, where required under law, if necessary to prevent or lessen a serious and imminent threat, and for certain types of research).
Unique identifiers	Are unique identifiers (eg. drivers licence number, Medicare number) being collected, used or disclosed? Has a new identifier been created (eg. an identifier composed of the person's initials and date of birth)? Is the provision or creation of a unique identifier necessary, done by consent, or authorised or required by law?
Direct / indirect collection	Will the information be collected directly from the individual or indirectly from a third party? Does the third party have authority to disclose? Does notice need to be given of any indirect collection?
Opting in / opting out	What opportunities will individuals have to consent or decline to provide certain information (including information not strictly necessary for the organisation's functions or activities), or to consent or object to particular uses?
Suppression	Will individuals have an opportunity to seek suppression of their identifying information where, eg. it is to be disseminated or published and they have concerns for personal safety?

Transparency (IPP 1.3 and 5)

Privacy policy	Does the organisation already have a privacy policy covering their collection and information handling practices? How often is this reviewed? Does it need to be amended in light of the new proposal?
Collection statement	Will individuals be informed of the reason/s their information is being collected, who it will be shared with and why, and that they have a right of access and correction? What form of privacy notice will be given and when?
Opportunity to object	Will individuals be able to object to the collection of certain types of information or particular uses and disclosures?

	If yes, will they be informed of this at the time of collection?
Notice of data matching arrangements	Where data matching is to occur, will the affected individuals be given prior notice of the fact and details of the proposed arrangement? Where their interests may be adversely affected, will individuals be given an opportunity to question the manner in which data has been processed to arrive at the adverse decision?
Consultation & publicity	Has or will the proposal be developed in conjunction with public consultation or be subject to Parliamentary or other scrutiny? Will the development or implementation of the proposal be publicised?

Access and correction (IPP 6; FoI Act)

FoI Act	Is the organisation holding the information required by the *Freedom of Information Act 1982 (Vic)* to give individuals access and the opportunity to correct their information*?*
Access from contracted service providers	Where the organisation uses contracted service providers, how will access requests be handled? Will the organisation maintain custody and control over the information? Will access be mediated by the organisation or handled directly by the contracted service provider?

Use and disclosure (IPP 2)

Primary use / disclosure	Is the intended use/disclosure in accordance with the primary purpose specified at the time of collection?
Reasonably expected uses / disclosures	What types of disclosure or uses would individuals reasonably expect? Will they be notified (at or around the time when their information is collected) of these related secondary uses/disclosures?
Authorised or required by law	Is the use or disclosure compelled or permitted by or under a statute or the common law? Is legislative amendment necessary to provide the necessary lawful authority, or to revise a statutory prohibition, for the use or disclosure?
Anticipating "function creep"	What other uses/disclosures are foreseeable now, at the time of collection, aside from the primary purpose for collection? How will notice be given of these uses/disclosures? As and when new, unanticipated or unrelated purposes arise, how would consent or other lawful authority be obtained?
Public interest uses/disclosures	Is there some public interest ground (in IPP 2.1) authorising use/disclosure (eg. public safety, research in the public interest,

	investigation of unlawful activity)?
Consensual uses / disclosure	Assume the project will use information already collected for some unrelated purpose. Is it practicable to seek consent for new uses/disclosures that were unanticipated or unrelated to the original reason for collection?
Data sharing	With whom will the information be shared? Does each participating organisation have the requisite lawful authority to collect or disclose the information? Is it necessary to share identifiable data? Is the data sharing necessary for the original or reasonably expected purpose notified to individuals at the time the information was originally collected? Has consent been obtained? Or, is the data sharing to be done for one of the designated public interests in IPPs 2 or 10?

Storage and disposal (IPP 4; Public Records Act)

Storage	Where will the information be maintained or stored, in paper or electronic form, by whom, and under what conditions?
Retention	How long will the information be kept before destruction or archiving? Should a minimum or maximum retention period be specified in advance?
Disposal	Is there a legislative requirement or contractual arrangement for disposing of the information? Is there an applicable disposal schedule under the *Public Records Act 1973 (Vic)*?
Destruction & de-identification	Is it lawful and practicable to de-identify (rather than destroy) the identifying information after a set period? To what extent is the information re-identifiable?

Data security (IPP 4)

Right to know	Who has a right or ability to access the information? Who has authority to access, change, add or delete information? Who authorises those access rights?
Need to know	Is access limited to only those individuals who need to have access to the information to carry out their roles? Is it necessary to limit the amount of information accessible to certain persons, depending on their role?

Security	Where information is to be stored or transmitted electronically or otherwise, how secure is the storage and method of transmission?
Deterrence / detection of misuse	How will the information be secured from internal and external misuse? How is misuse deterred and, if it were to occur, how is it detected?

Data quality (IPP 3)

Reliable equipment	Where technology is to be used to gather or process information, how reliable is the equipment? Is it periodically tested for accuracy? Are audit trails and other records generated of adequate quality, and do they contain sufficient information for their intended use?
Reviewing data quality	Is it necessary to ensure that information is reviewed periodically to ensure it is accurate, complete and up to date? Review how often, having regard to the particular information, its uses and its consequences for the individuals it relates to?

Due diligence (s 68)

Training	What sort of precautions (eg. training, procedures manuals and other awareness-raising initiatives) can be taken to minimise the risk that the organisation's employees will misuse information?
Audit trails	Is the flow of information tracked so that any misuse is likely to be detected and deterred? Are employees given notice of this tracking, both for their own sake and in order to deter misuse?
Sanctions for misuse	Are there clear and enforceable legislative, disciplinary or other sanctions for misuse?

Accountability and review

Independent oversight	Is the proposal subject to an effective and independent oversight mechanism responsible for ensuring, promoting and reporting on compliance?
Cross-border oversight	Where the proposal involves the sharing of data across public and private sectors, or across jurisdictions, is there a designated accountability person or body, responsible for oversight of the whole system (including review, audit and investigation, reporting, and complaints and redress)?
Public reporting	Should the fact and operation of the proposal be made public? Is it desirable for the extent and manner of information collection and handling to be reported on to the relevant Minister, to Parliament or to the community?
Investigation & audit	Will the project be audited to ensure it complies with data protection standards? Who will carry out the audits, and how often?
Complaints & redress	Where individuals have concerns about how their information is handled, where can they complain? Who is responsible for handling complaints and providing redress? What redress is available to remedy a complaint that has caused harm?
Review	When, and how often, is the project to be reviewed and assessed to determine whether it is achieving its stated aims? Who will conduct the review? Will they be properly independent? Will the review and/or its results be made public?
Sunset	Should the proposal cease after a set time? Is it to be implemented to achieve a short-term goal? Is the need for it likely to fade or be superseded? Should the proposal continue (whether or not in modified form) only after it has been assessed and subjected to fresh approval? If so, by whom? When?

Resource 2: how others do it

The following list of PIA resources include guides, worksheets, and case studies undertaken in Australian and overseas jurisdictions. In some cases, PIAs are required under either statute (eg the USA's *E-Government Act of 2002* and Alberta, Canada's *Health Information Act*, which came into force in 2001) or policy direction (eg the Canadian Government's *PIA Policy* introduced in May 2002). In most cases, PIAs are recommended for major projects and initiatives.

Asia & Pacific

Australia

Federal

Australia, Office of the Federal Privacy Commissioner, "Framework for Assessing Law Enforcement Initiatives where they Impact on Privacy" in *Preserving Privacy in a Rapidly Changing Environment*, presentation to the Fourth National Outlook Symposium on Crime in Australia, "New Crimes or New Responses", convened by the Australian Institute of Criminology in Canberra on 21 June 2001
http://www.privacy.gov.au/news/speeches/sp34note.pdf

Australia, Office of the Federal Privacy Commissioner, "Content of data-matching program protocols", "Sample program protocol" and "Technical standards report" in Appendices A-D of the *The Use of Data Matching in Commonwealth Administration – Guidelines*, February 1998
http://www.privacy.gov.au/publications/p6_4_23.doc

Example:

Australia, Office of the Federal Privacy Commissioner, "Privacy Impact Assessments (PIA)", appendix 1 in *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to Communicate or Transact with Individuals*, December 2001
http://www.privacy.gov.au/publications/pki.pdf

Victoria

Australia, Victoria, Department of Human Services, "System Development Privacy Assessment – Model System Development" and "RARF – Privacy Impact Assessment", *Risk Assessment and Response Framework (RARF)*, last updated November 2003
http://www.dhs.vic.gov.au/privacy/html/compliance_tools/index.htm
http://www.dhs.vic.gov.au/privacy/downloads/xls/modelsystem.xls
http://www.dhs.vic.gov.au/privacy/downloads/xls/model_pia.xls

New Zealand

New Zealand, Office of the Privacy Commissioner, *Privacy Assessment Handbook*, March 2002
www.privacy.org.nz/comply/pia.html

New Zealand, Office of the Privacy Commissioner, *Guidance Note for Departments Seeking Legislative Provision for Information Matching: Information Matching Privacy Impact Assessments*, January 1999
http://www.privacy.org.nz/comply/impia.html

Examples:

Philippa Fogarty, *Privacy Impact Assessment in Respect of the Justice Data Warehouse*, prepared for the NZ Ministry of Justice, June 2002, revisions added June 2003
http://www.jsis.govt.nz/Public/data-warehouse/pia-revised-2003/privacy-impact-assessment-2003-revision.htm

John Edwards, *Privacy Impact Assessment in Respect of a Proposal to Develop a National Student Index Number*, prepared for the NZ Ministry of Education, December 2000
http://www.minedu.govt.nz/web/downloadable/dl5720_v1/final-formatted-pia-january-2001.doc

New Zealand, State Services Commission, E-government Unit, *Preliminary Privacy Impact Assessment of Models being Considered for Inclusion in a Proposal for Online Authentication for E-Government*, version 0.9, March 2003
http://www.e-government.govt.nz/docs/authent-pia-prelim/authent-pia-prelim.pdf

Pacific Privacy Consulting in association with Xamax Consultancy, *Authentication for E-Government: Privacy Impact Assessment Report*, prepared for E-government Unit, State Services Commission, New Zealand, December 2003
http://www.e.govt.nz/docs/authent-pia-200312/authent-pia-200312.pdf

Statistics New Zealand, *Injury Statistics Project Pilot: Privacy Impact Assessment*, May 2004
http://www.stats.govt.nz/domino/external/web/Prod_Serv.nsf/Response/Injury+Statistics+Releases+and+Reports

Statistics New Zealand, *Linked Employer-Employee Data Project: Privacy Impact Assessment*, September 2003
http://www.stats.govt.nz/domino/external/web/prod_serv.nsf/Response/LEED+Reports

Hong Kong

Examples:

Hong Kong, Legislative Council, Panel on Security of the Legislative Council, *HKSAR Identity Card Project – Initial Privacy Assessment Report*, February 2001, LC Paper No. CB(2)752/00-01(04) and *HKSAR Identity Card Project – Latest developments and the Second Privacy Impact Assessment Report*, June 2002, LC Paper No. CB(2)2433/01-02(07)
http://www.legco.gov.hk/yr03-04/english/panels/se/papers/se_h.htm

The Americas

Canada

Federal

Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy and Privacy Impact Assessment Guidelines: A Framework for Managing Privacy Risks*, May 2002
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp

Treasury Board of Canada Secretariat, *Privacy Impact Assessment e-Learning Tool*, last updated October 2003
http://www.cio-dpi.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp

Alberta

Canada, Office of the Information and Privacy Commissioner of Alberta, *Privacy Impact Template*, January 2001
http://www.oipc.ab.ca/pia/template.cfm

Examples:

Canada, Office of the Information and Privacy Commissioner of Alberta, *Privacy Impact Assessment Registry* (searchable registry of PIAs submitted by public bodies and custodians to, and accepted by, the OIPC), ongoing
http://www.oipc.ab.ca/pia/registry.cfm

British Columbia

Canada, British Columbia, Ministry of Management Services, Privacy and Information Access Branch, *Privacy Impact Assessment Process*, last updated November 2003
http://www.mser.gov.bc.ca/foi_pop/PIA/PIAprocess.htm

Ontario

Canada, Government of Ontario, Management Board Secretariat, Information and Privacy Office, *Privacy Impact Assessment: A User's Guide*, updated June 2001
http://www.gov.on.ca/MBS/english/fip/pia/index.html

Canada, Government of Ontario, Management Board Secretariat, Access and Privacy Office, *Model Cross-Jurisdictional Privacy Impact Assessment Guide - Draft*, October 1999
http://www.gov.on.ca/mbs/english/fip/pub/fed_pia.pdf

Examples:

Canada, Information and Privacy Commissioner of Ontario, and Advanced Card Technology Association of Canada, *Smart, Optical and Other Advanced Cards: How to do a Privacy Assessment*, September 1997
http://www.ipc.on.ca/docs/cards.pdf

Canada, Information and Privacy Commissioner of Ontario, and Advanced Card Technology Association of Canada, *Multi-Application Smart Cards: How to do a Privacy Assessment*, August 2000
http://www.ipc.on.ca/docs/multiapp.pdf

Canada, Information and Privacy Commissioner of Ontario, *Geographical Information Systems*, see Appendix A ("Privacy Impact Assessment"), April 1997
http://www.ipc.on.ca/scripts/search.asp?action=98&RefAct=31&P_ID=11405&N_ID=1&PT_ID=11351&U_ID=0

Saskatchewan

Canada, Office of the Saskatchewan Information and Privacy Commissioner, *Introduction to the Privacy Impact Assessment* and *Privacy Impact Assessment (Short Form)*, April 2004
http://www.oipc.sk.ca/Web%20Site%20Documents/PIA Intro -- Official Version -- April, 2004.pdf
and
http://www.oipc.sk.ca/Web Site Documents/PIA Short Form -- Official Version April, 2004.pdf

USA

United States, Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum for Heads of Executive Departments and Agencies, M-03-22, September 2003
http://www.whitehouse.gov/omb/memoranda/m03-22.html

United States, Department of the Interior, Office of the Chief Information Officer, *Privacy Impact Assessment and Guide* and *Privacy Impact Assessment Template*, March 2004
http://www.doi.gov/ocio/privacy/pia.htm

Examples:

US Department of Justice, in co-operation with the Office of the Ontario Information and Privacy Commissioner, *Privacy Impact Assessment for Justice Information Systems Working Paper*, February 2001
http://www.ojp.usdoj.gov/archive/topics/integratedjustice/welcome.html

United States, National Criminal Justice Association, *Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*, September 2002
http://www.ncja.org/pdf/privacyguideline.pdf

US Internal Revenue Service, *IRS Privacy Impact Assessment*, December 1996, endorsed by Federal Chief Information Officers Council in 2000
http://www.cio.gov/archive/pia_for_it_irs_model.pdf

Europe

European Commission

Cap Gemini UK plc, *IDA [Interchange of Data between Administrations] Programme: A Guide to Data Protection Compliance*, version 1, study sponsored by the European Commission, March 1998
http://en.infosoc.gr/content/downloads/data_protection_compliance.pdf

United Kingdom

United Kingdom, Cabinet Office, Performance and Innovation Unit, "The Analytical Framework and Privacy Impact Assessments", Annex D in *Privacy and Data-Sharing: The Way Forward for Public Services*, April 2002
http://www.number-10.gov.uk/su/privacy/annex-d.htm

United Kingdom, Department for Constitutional Affairs, *Public Sector Data Sharing: Guidance on the Law*, esp Appendices 1 ("Is Data Sharing Intra Vires?") 2 ("Relevant Considerations for Lawful Sharing of Personal Data") and 3 ("Checklist of Relevant Legal Considerations Relating to Data Sharing Partnerships"), November 2003
http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.pdf

Examples:

United Kingdom, Department for Constitutional Affairs, *Case Studies [illustrating application of legal guidance to data sharing]: (1) Community Incident Action Groups; (2) Electronically Sharing Client Data Pilot Scheme; (3) The Connexions Service; and (4) Bolton Information Sharing and Assessment Pilot Project*, undated
http://www.dca.gov.uk/foi/sharing/toolkit/casestudies.htm

Non-Government

International Biometric Group's BioPrivacy Initiative, *BioPrivacy Application Impact Framework*, 2000-2003
http://www.bioprivacy.org/index.htm

Thomas J. Karol (Deloitte & Touche), *A Guide to Cross-Border Privacy Impact Assessments*, commissioned by the IT Governance Institute and the Information Systems Audit and Control Foundation Research Board, 2001
http://www.itgi.org/ContentManagement/ContentDisplay.cfm?ContentID=7404

Resource 3: the Information Privacy Principles

SCHEDULE 1 of the Information Privacy Act 2000

THE INFORMATION PRIVACY PRINCIPLES

In these Principles –

"sensitive information" means information or an opinion about an individual's –

(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual preferences or practices; or
(ix) criminal record –

that is also personal information;

"unique identifier" means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name.

1. Principle 1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of –

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. Principle 2 Use and Disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless –

(a) both of the following apply –

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual –

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information; or

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent –

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety, or public welfare; or

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(f) the use or disclosure is required or authorised by or under law; or

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(h) the Australian Security Intelligence Organization (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and –

(i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and

(ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(g), it must make a written note of the use or disclosure.

3. Principle 3 Data Quality

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

4. Principle 4 Data Security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

5. Principle 5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Principle 6 Access and Correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that –

(a) providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders –

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (j) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, the organisation –

(a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and

(b) may refuse access to the personal information until the fee is paid.

6.5 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 must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must –

(a) provide access, or reasons for the denial of access; or

(b) correct the personal information, or provide reasons for the refusal to correct the personal information; or

(c) provide reasons for the delay in responding to the request for access to or for the correction of personal information--

as soon as practicable, but no later than 45 days after receiving the request.

7. Principle 7 Unique Identifiers

7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.

7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless –

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless –

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or

(b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8. Principle 8 Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9. Principle 9 Transborder Data Flows

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if –

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply –

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

10. Principle 10 Sensitive Information

10.1 An organisation must not collect sensitive information about an individual unless –

(a) the individual has consented; or

(b) the collection is required under law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns –

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if –

(a) the collection –

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

Privacy Victoria Publications at August 2004

Copies of publications produced by Privacy Victoria are available through the Office or from our website at www.privacy.vic.gov.au. Requests for copies may also be made to enquiries@privacy.vic.gov.au or by telephoning 1300 666 444.

Guidelines

How to prepare for the *Information Privacy Act 2000*, *May 2002*
Guidelines to the Information Privacy Principles – Part One, *May 2002*
Guidelines to the Information Privacy Principles – Part Two, *August 2002*
Website Privacy – Guidelines for the Victorian Public Sector, *May 2004*

Issue Papers

Issue Paper 01.02
Public Registers and Privacy: Building Permit Data, *January 2002*

Reports

Report 01.02

Public Registers and Privacy: Building Permit Data - a report to the Minister for Local Government, *August 2002*

Report 02.02

Privacy in Diverse Victoria - attitudes towards information privacy among selected Non-English speaking background and Indigenous groups in Victoria, *October 2002*

Procedures & Guides

Procedure for Service of Compliance Notices under section 44 of *the Information Privacy Act, July 2003*

Information Sheets

01.02 Regulation of Online Content – Child Porn
02.02 Privacy and School Reports
03.02 Frequently Asked Questions – Public Sector
04.02 Victoria's Privacy Protection Landscape
05.02 Complaint Handling Under the *Information Privacy Act*
06.02 Email Disclaimers and Privacy
07.02 A Brief History of Information Privacy
08.02 Dogs, Cats and their Owner's Privacy
09.02 Comparative Table of Organisations' Responsibilities under Australian Privacy Legislation
10.02 Fences and Privacy
11.02 Bushfires and Privacy
12.02 Frequently Asked Questions – General Public
01.03 Images and Privacy
02.03 Property Sales, Valuers and Privacy
03.03 Privacy Regulation Across Australia (at 30 June 2003)
04.03 International Privacy Standards
05.03 Mobile Phones with Cameras
01.04 Privacy Regulation Across Australia (at 30 June 2004)
02.04 Access and Correction Rights and your Personal Information

Case Notes

A v Local Council [2002] VicPCmr1
B v Victorian Government organisation [2003] VicPCmr2
Complainant v Statutory Entity Respondent [2004] VicPCmr3
Complainant v Department Respondent [2004] VicPCmr4
Complainant v Local Council Respondent [2004] VicPCmr5
Complainant v Department Respondent [2004] VicPCmr6
Complainant v University Respondent [2004] VicPCmr7
Complainant v Statutory Entity Respondent [2004] VicPCmr8
Complainant v Minister Respondent [2004] VicPCmr9
Complainant v Department Respondent [2004] VicPCmr10

Guides to Complaint Handling

- Guide for Complainants under the IPA
- Guide for Respondents under the IPA
- Conciliation under the IPA
- Complaint handling under the IPA
- Guide to the Handling of Complaints under the IPA by the Victorian Civil and Administrative Tribunal