Privacy Commissioner
Te Mana Matapono Matatapu

PRIVACY IMPACT ASSESSMENT HANDBOOK

Contents

Foreword by the Privacy Commissioner

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 can achieve my objectives while also protecting privacy?

This handbook provides the tools to help to answer these questions.

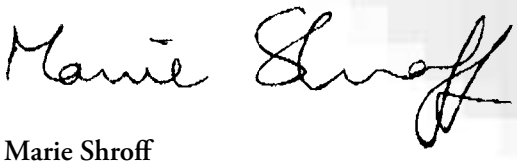
Protection of privacy is more than simply avoiding a breach of the law. It can involve striving for something better. Privacy impact assessment is one of a range of new techniques which are increasingly being used internationally to better manage privacy risks. Others include privacy compliance audits, 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 than an intrusive one, if the option is identified sufficiently early in project planning.

Privacy impact assessment is being encouraged in Hong Kong, Canada and Australia as a means by which business and government can proactively identify and avoid privacy problems. In Hong Kong, privacy impact assessment is an important part of a policy approach to building trust and confidence in e-business. In Australia the process is recommended as part of any new Public Key Infrastructure system. A number of Canadian governments, federal and provincial, have or are developing policies requiring privacy impact assessment to be undertaken on new projects. The Province of Alberta has gone one step further and requires by law privacy impact assessments to be undertaken before establishing new public health information systems. A number of American institutions, including the Internal Revenue Service, have adopted internal policies requiring the use of privacy impact assessment.

Privacy impact assessment is seen internationally as a valuable tool for businesses and governments which take privacy seriously.

I commend New Zealand organisations to employ privacy impact assessment for significant new initiatives involving the handling of personal information. Achieving and maintaining public trust in electronic service delivery is a key challenge for e-government and e-commerce. Failure to give informed consideration to privacy issues when embarking on new projects could be an expensive mistake. A privacy impact report will fill a gap in the knowledge of decision makers and enable them fully to get to grips with the issues at the right time - before decisions are taken.



Marie Shroff

PRIVACY COMMISSIONER

1. Overview

Privacy Impact Assessment (PIA) is a systematic process for evaluating a proposal in terms of its impact upon privacy. PIA helps an agency to:

- identify the potential effects that a proposal may have upon individual privacy
- examine how any detrimental effects upon privacy might be overcome
- ensure that new projects comply with the information privacy principles.

The contents of this handbook will be of particular value to those who are not IT specialists but have organisational responsibility for complying with data protection and privacy laws and policies. The handbook's objectives are:

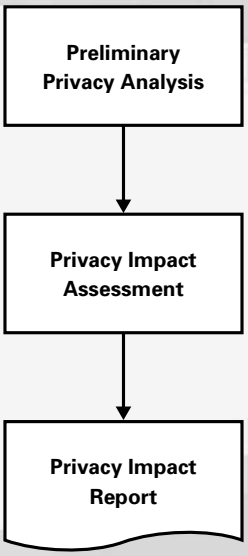
- to explain the benefits of **Privacy Impact Assessment** (PIA) for public and private agencies involved in projects with significant potential impact upon privacy
- to offer a framework to enable PIA to be undertaken appropriately and effectively
- to help assessors to prepare consistent, structured, high quality privacy impact reports.

The comments and suggestions in this handbook are particularly suited to projects with a technological component, especially e-commerce and e-government initiatives. However, the booklet may also help businesses, government departments and others operating off-line. The handbook is not intended to offer legal advice about the interpretation of the **Privacy Act 1993** ("the Act").

Privacy Impact Assessment is a technique that should be useful to any public or private sector agency that handles personal information, particularly medium to large businesses and government departments. There are distinct advantages in outsourcing the preparation of a privacy impact report to lend impartiality to the process. That may be critical in influencing consumer or public opinion. Nonetheless, it is feasible to undertake PIA in-house, using the skills and experience of the project team and the wider organisation.

This handbook provides detailed practical guidance on how to prepare a privacy impact report:

- *Preliminary privacy analysis* – is a PIA needed for this project?
- *Terms of reference* – setting the task for the assessment.
- *Describing the project and information flows* – accurately understanding, and clearly describing, the processes is essential before analysing the privacy risks.
- *Privacy analysis* – examining all aspects of the proposed system from obtaining to destruction of data.
- *Privacy risk assessment* – identify the risks and judge their nature and seriousness.
- *Privacy enhancing responses* – security safeguards, privacy enhancing technologies and other management and technological solutions.
- *Compliance mechanisms* – ensure that responses are effective in operation and trigger action if change occurs or if the measures implemented prove ineffective.



Privacy impact assessment provides an "early warning system" for agencies. The PIA radar screen will enable an organisation to spot a privacy problem and take effective counter-measures before that problem strikes the business as a privacy crisis. The process can help by:

- providing credible information upon which business decisions can be based
- saving money by identifying privacy issues early, at the design stage
- enabling organisations to identify and deal with their own problems internally and proactively rather than awaiting customer complaints, external intervention or a bad press.

Proper assessment can make an initiative privacy enhancing without compromising business objectives or adding significant costs. PIA is a technique for any business or public body that is serious about the need to maintain customer trust and confidence.

2. The Information Privacy Principles

The Privacy Act sets out 12 information privacy principles ("IPPs") – see Appendix A. Agencies must comply with those provisions.

The IPPs are based upon international principles of fair information practice. Similar principles form the backbone of privacy and data protection legislation in an increasing number of jurisdictions throughout the world. The principles apply to the collection, accuracy, use, disclosure and security of personal information. They also provide for access to, and correction of, personal information and place controls on unique identifiers.

The IPPs impose duties upon agencies, and confer rights upon individuals, in relation to personal information. Their coverage can be discerned from their general headings:

- **principle 1** – purpose of collection of personal information
- **principle 2** – source of personal of information
- **principle 3** – collection of information from subject
- **principle 4** – manner of collection of personal information
- **principle 5** – storage and security of personal information
- **principle 6** – access to personal information
- **principle 7** – correction of personal information
- **principle 8** – accuracy, etc, of personal information to be checked before use
- **principle 9** – agency not to keep personal information for longer than necessary
- **principle 10** – limits on use of personal information
- **principle 11** – limits on disclosure of personal information
- **principle 12** – unique identifiers.

In addition to the IPPs, which are relevant to all the handling of personal information by agencies, the Act contains other sets of principles, guidelines and rules applicable in certain circumstances. These include the public register privacy principles and the information matching guidelines and rules.

This handbook does not discuss the specifics of the IPPs or the other statutory principles, guidelines and rules. However, there are a number of readily available resources on the Privacy Act – see Appendix B. Information can also be obtained by consulting the Privacy Commissioner's website or by telephoning the privacy enquiries line (0800 803 909).

3. *What* Is Privacy Impact Assessment?

The Privacy Act does not define privacy impact assessment and it is a concept that continues to evolve. The International Association for Impact Assessment defines impact assessment as "the identification of future consequence of a current or proposed action". For the purposes of this handbook, PIA is described as a systematic process that evaluates a proposal in terms of its impact upon privacy.

To be effective, PIA needs to be an integral part of the project planning process rather than an afterthought. The purpose of the assessment is to:

- identify the potential effects that the proposal may have upon personal privacy
- examine how any detrimental effects on privacy might be lessened.

PIA may be applied to a wide range of projects. It applies to any proposal that could intrude on reasonable expectations of privacy or the rights enshrined in the Act. It can be used with a public policy initiative or a corporate project.

A privacy impact report seeks to identify and record the essential components of any proposed system containing significant amounts of personal information and to establish how the privacy risks associated with that system can be managed. A PIA will sometimes go beyond an assessment of a "system" and consider critical "downstream" effects on people who are affected in some way by the proposal.

PIA can be distinguished from privacy compliance audits. Privacy compliance audits are carried out on existing systems to ensure their conformity with internal rules and external requirements in relation to privacy and data protection. By contrast, PIA focuses on understanding a proposed system (or the effects of proposed change to an existing system). The aim is to identify and reduce future adverse impacts as well as to inform decision-makers about whether a project should proceed and, if so, in what form. However, the distinction is not absolute and there may be a useful inter-relationship between the different techniques. For example, the results of a privacy compliance audit on an existing system would be a valuable resource for anyone undertaking a PIA on proposed enhancements or changes to that system.

4. *Why* Undertake Privacy Impact Assessment?

Privacy Impact Assessment can operate as an "early warning system" for businesses and government organisations. It can help management make better informed decisions and avoid a privacy disaster. No chief executive wants to see his or her organisation's exciting new product or initiative panned in the news media as a danger to customer privacy. While favourable publicity can never be guaranteed, acting on a privacy impact report improves the chances that any privacy headlines are good news for the business rather than a public relations (and possibly share price) disaster.

PIA can help public and private sector agencies in a number of ways:

- PIA offers a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers. PIA can provide a credible source of information by assuaging alarmist fears or alerting the complacent to potential pitfalls.
- In some cases bitter consumer and public reaction has led to the withdrawal of a new and expensively developed product for privacy reasons. PIA ensures that a business is the first to find out about privacy pitfalls in its project, rather than learning of them from critics or competitors. A privacy impact report can save money and protect reputation.
- PIA brings privacy responsibility clearly back to the proponent of a proposal. They must "own" any problems and devise appropriate responses in the design and planning phases. It also ensures that divisions within larger businesses recognise that their projects must not jeopardise the trust vested in the wider business.
- PIA encourages cost-effective solutions, since it is cheaper to do things at the design phase to meet privacy concerns than attempt to retrofit after a system is operational.
- PIA can make the difference between an invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs.
- The Privacy Commissioner can add value to the process by reviewing a privacy impact report, rather than having to investigate the practices of the business itself. This is cost effective for the Commissioner and less intrusive for a business.

Significant risks to privacy exist in e-commerce and e-government. These risks must be confronted if trust and confidence are to prevail in the relationships with consumers and citizens. Until the hallmarks of trust and confidence are reflected in community perceptions, electronic service delivery will be impeded in realising its full potential.

5. *Who* Should Undertake Privacy Impact Assessment?

PIA is a technique that can be used by any agency handling personal information. The technique is especially suited to medium to large businesses and to government departments.

A variety of skills are required for undertaking an assessment and completing a privacy impact report, but a single individual need not possess them all. The person undertaking the assessment needs to have sound analytical and writing skills. He or she also needs to be familiar with information privacy and data protection approaches and analysis and the IPPs. If not personally possessing relevant technical skills or experience, the assessor would need to be able to absorb the paperwork associated with the project and to have an ability to get alongside technical people, to ask pertinent questions, be able to understand the answers and translate them into a report that can be understood by others. An enquiring mind and a talent for "lateral" thinking are valuable.

The person undertaking the assessment and writing the report will draw on the skills of others. Depending upon the nature the project, the range of necessary skills might include:

- *Policy development skills* – including business-specific policy experience, broad strategic policy and planning skills and consultation skills.
- *Operational programme and business design skills* – to examine proposals for the operational flow of the business, and analyse the feasibility, practicality, and efficiency of relevant aspects of the project and the responses to the privacy risks.
- *Technology and systems expertise* – in the design attributes and operation of, for instance, mainframe and legacy systems, networking products, new Internet tools, system security, customer interface systems, financial or transactional settlement systems, or biometric tools.
- *Risk and compliance analysis skills* - such as those associated with comprehensive financial and due diligence audits, and the emerging specialties related to computer system vulnerabilities.
- *Procedural and legal skills* – relating to project authority, use of personal information, legal and institutional oversight mechanisms, statutory, regulatory and contractual options and potential legislative conflicts where several laws or jurisdictions are involved.
- *Information privacy and data protection expertise* – relating to the Act, national or sectoral privacy laws in other jurisdictions, privacy provisions in relevant applicable statutes, national and international privacy standards, privacy enhancing technologies and current privacy developments.

Unless people with the right competencies are used, it is likely that the assessment process will be more difficult and protracted than necessary. The resulting analysis and conclusions may be less sound or insightful.

There will be a number of choices available to the business about who will carry out the PIA. Sometimes most of the necessary skills will reside in the team assembled to develop the project itself. Experts with particular skills may be brought in to assist with certain aspects. An agency's Privacy Officer may undertake a coordinating or checking role.

Competent privacy expertise can be accessed in New Zealand and Australia and may be brought in even when most of the work will be done by the project team. The assessor will work closely alongside the project team to fully understand the business, the project, the risks and the appropriate responses. Where the PIA is solely undertaken internally, thought should be given to incorporating some external or independent oversight. One possibility is to use a privacy or data protection consultant to carry out such a check.

Another is to show the privacy impact report or a draft version of it to the Office of the Privacy Commissioner. While this is routinely done with government departments, a business intending to do so should discuss the matter in advance since the Commissioner may not be willing to consider the report on a confidential basis (the office is, for instance, subject to the Official Information Act 1982). Typically the Privacy Commissioner will be willing to receive a PIA for information only and will have staff offer some feedback and constructive suggestions. If any of the content is commercially sensitive or otherwise confidential, this should be clearly marked. Showing the privacy impact report to the Commissioner does not affect an agency's obligation to comply with the Act, but the organisation will be seen as a responsible corporate citizen making diligent efforts to identify and mitigate privacy risks.

Certain projects will have significant privacy implications in more than one jurisdiction. Indeed, some initiatives will have truly global implications. In such cases, comment might be invited from the privacy commissioners of several countries before finalising the privacy impact report. A significant objective of a PIA in such projects may be to ensure that the project meets or exceeds the data protection and information privacy requirements in all the relevant countries and achieves a level of trust amongst consumers and regulators.

Occasionally the business that will ultimately use the proposed system will not itself undertake or commission the PIA. For instance, a software development company might commission an assessment of a new business computer program which will be made available commercially for others to use. In other cases a government body, an industry group, or an association of several organisations might commission a PIA for a project that may affect a number of businesses (such as a credit reporting system to be used by credit providers or a public health database into which medical practitioners might provide data). In these cases the PIA will contribute to solutions from which many businesses may benefit and to the trust which each needs in order to confidently share data.

If the planned projects are very similar, government departments, or affiliated businesses, should consider undertaking a generic or overarching PIA to avoid unnecessary duplication of effort.

6. *Which* Projects Warrant Privacy Impact Assessment?

Some projects are of such a scale or nature that there is a clear need for a PIA. For example, a data-warehouse holding personal information on nearly all people in New Zealand would be an obvious candidate. Similarly, the application of cutting edge technology to an aspect of data processing where the effects are not widely understood or trusted by the public (for instance, requiring customers to undergo biometric identification to access a service). In other cases, the surveillance capacity or intrusiveness may be of such a nature as to make the merits of a PIA seem obvious. Virtually any project which will amass otherwise confidential information into accessible databases are prime candidates for a PIA – and the technique has proved especially useful in the context of public health initiatives.

However, there will be many other more mundane, but nonetheless significant projects, which will benefit from PIA. For example:

- merging internal business databases to enable new forms of client profiling
- centralising a multi-national company's employee records in New Zealand or elsewhere
- changing the way information is collected in customer interface systems (for instance, adopting unattended kiosks, automated voice responses, smartcards, remote access tools).

PIA may be desirable to assess and address risks:

- arising from a new technology or the convergence of existing technologies (for instance, intelligent transportation systems, person-location or person-tracking using cellphone or GPS technologies, combining face-recognition and CCTV)
- where a known privacy-intrusive technology is to be used in new circumstances (for instance, expanding data matching or drug testing, installing video surveillance in a workplace)
- in a major endeavour or change in practice with significant privacy effects (for example, the merging of major public registries into a "super registry", the adoption of new forms of required ID, shared access to other organisations' electronic data bases).

As part of a wider business privacy strategy, a business may adopt a PIA policy. A policy might include requiring a privacy impact report for new programmes or systems that involve significant collection, use or disclosure of personal information. Such a policy should also include a PIA for major changes to existing programmes. It would be unnecessary to undertake an assessment for minor changes to existing programmes or systems.

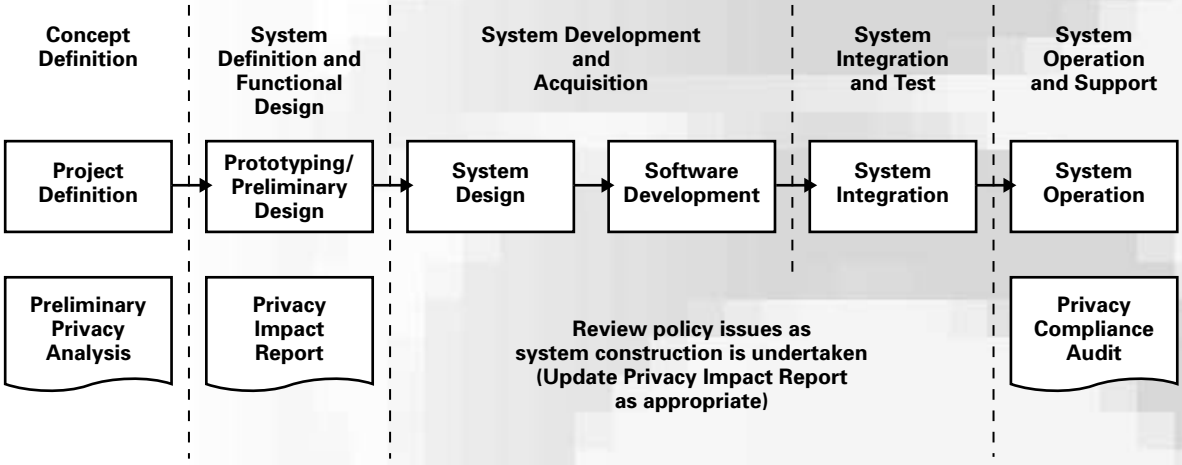
An organisation which intends to use assessment as an ongoing privacy management tool should establish a process for determining when a privacy impact report is required. This might include, for example, involving the organisation's Privacy Officer. It would also be feasible to prepare internal PIA templates or questionnaires tailored to the nature of the business and its internal policies.

7. *When* To Undertake Privacy Impact Assessment?

The ability to design system architecture which addresses actual or potential privacy concerns is dependent, to some extent, on early identification of privacy issues and risks. An understanding of the kinds of questions that will arise in the context of PIA, as well as a sense of where risk may lie, should therefore be incorporated into the early phases of the project and system development.

Ideally, full and detailed consideration of privacy issues should precede system design. However, sometimes it may only be possible to complete a PIA at later stages in the system development and acquisition phase. If so, the privacy impact report can be an evolving document which will become more detailed over time. Thus, even at the early stages in the diagram below, consideration may be given to the sources of potential risk. Responses can be refined in revised versions of the privacy impact report.

The Privacy Impact Assessment and the Systems Development Life Cycle



The early phase, prior to formally undertaking a PIA, may be referred to as preliminary privacy analysis. At this point, an attempt should be made to briefly document key features of the project and issues which have been identified without detailed study. Preliminary privacy analysis can assist by:

- informing the decision whether to prepare a privacy impact report
- defining resource requirements (such as the skills that might be needed by an assessor, whether the task is small or large)
- suggesting terms of reference for the assessment
- providing a tool for initiating consultation with the Privacy Commissioner.

8. *How* To Undertake Privacy Impact Assessment?

Once the organisation has undertaken a preliminary privacy analysis, selected a suitable person to prepare the report and drafted the terms of reference, it is ready to begin the assessment.

The terms of reference will describe the project to be assessed and explain how that should be integrated into the project timeline (for example, setting deadlines for the privacy impact report which fit with key project milestones). Sometimes the terms of reference will be fairly open-ended. In other cases it may be desirable to focus the assessment on particular aspects or to rule in or out particular alternatives. The terms of reference may also list resource people to whom the assessor should refer.

If the organisation does not have a clear practice on such matters, the terms of reference could also set out how a report is to be dealt with (for example, whether a draft should be provided to the Privacy Commissioner for comment and whether the completed privacy impact report will be made publicly available). Usually, there is merit in making completed privacy impact reports publicly available and organisations should consider posting the privacy impact report or a summary on their website. Openness about the findings can contribute to the maintenance of public trust and confidence in the organisation and can ensure that its practices and policies in relation to the handling of personal information are fair and freely available.

9. Elements Of A Privacy Impact Report

There are a number of common elements that each PIA needs to cover. A table of contents for a typical privacy impact report is suggested below. A more detailed discussion of the contents follows, with suggestions about matters to be addressed and questions to be answered. It can be used as a checklist.

TABLE OF CONTENTS FOR A TYPICAL PRIVACY IMPACT REPORT

The questions and prompts below should be seen merely as a starting point: the subject matter of a particular project will suggest other matters that ought to be addressed. Some questions will not be relevant to a particular project and the privacy impact report should expressly state this (for instance, explaining that a proposal will not involve the use of any unique identifiers or transfers of information out of New Zealand).

A. INTRODUCTION AND OVERVIEW

A privacy impact report needs to be written in such a way that it will easily be understood by non-technical people. The report will be read by managers, decision-makers and stakeholders. The introduction will explain the assessment process undertaken and introduce readers to the structure of the report.

The overview may be the opportunity to explain aspects of the organisation's privacy management. It might outline a company's privacy policies or commitment to good standards of data protection. If it is a large organisation, the overview might explain relevant parts of the corporate structure. A public body might outline relevant statutory authorisations or constraints. The role and involvement of the Privacy Officer might be explained. Any reporting processes existing to ensure that management is informed of privacy issues could be outlined. The privacy impact report may be part of that process.

The privacy impact report should include certain basic details such as the identities of the authors, the date of the document and a glossary of any special terms used. It will also be useful to explain any assumptions underlying the assessment and set out the terms of reference.

B. DESCRIPTION OF THE PROJECT AND INFORMATION FLOWS

A careful and accurate description of the project is of tremendous importance in a privacy impact report. Preparing good descriptive material can be challenging, since technical systems-specifications will need to be translated into ordinary language. It is important that the description remains accurate and is sufficiently precise and detailed. Appropriate flow charts can be extremely valuable.

Some suggestions:

- Provide a summary of the project including a description of the needs that led to it.
- Describe the information to be used in the project.
- Provide diagrams depicting the flow of personal information. The flow charts should clearly illustrate how data is collected or obtained, how it circulates internally and how it is disseminated beyond the organisation. Supplementary flow charts might be useful to illustrate particular aspects such as access control and retention/destruction practices.
- Explain who will have access to particular categories of personal information. Such explanations or diagrams will illustrate a "need to know" approach.

C. THE PRIVACY ANALYSIS

The privacy analysis will follow the information "life cycle" of collection and obtaining of personal information, through its use, retention, processing, disclosure and destruction. It will highlight how the project changes any previous information handling practice and how this may affect individuals. Although the analysis should not usually seek to present a legal opinion, it should highlight any area where there might be a problem in compliance with the IPPs. The report should not limit itself to compliance issues and should discuss and analyse the proposal with respect to the potential advantages and risks in information privacy terms and identify best practice wherever possible.

The privacy analysis may work through issues of information collection and obtaining, then use, disclosure and retention of personal information, with a further section on risk assessment. This approach is simply one of several that are equally worthwhile. It is perfectly acceptable to integrate privacy risk assessment into the discussions of collection, use, disclosure and retention.

Naturally, the approach will be adapted to the issues at stake. In some cases the emphasis will be on only one or two issues.

Collecting and obtaining information

- Describe the personal information that is collected or obtained.
- Indicate the source of each item of information.
- Describe what information will be collected directly from the individual. Explain the circumstances and means of collecting (for instance, whether information is collected as part of an existing activity or transaction or whether there will be a specific collection for the purposes of the project).
- Explain aspects of the project that are directed towards compliance with IPPs 1-4.
- Where the information is collected as part of an existing process, explain the purposes for which information is currently obtained and how these will be changed as a result of the project.
- Where the purposes differ from the current purposes, outline how the individuals concerned will be made aware of the new purposes. Might individuals be surprised or concerned by the new purposes? Is there any sensitivity associated with the collection directly from the individual through an existing process? Will it be mandatory or voluntary?

- If information is to be collected from someone other than the individual concerned or obtained from some other database or source, explain how this is proposed to be done. Where information is to be obtained from an existing database, list the purposes for which information is held in that database and explain the extent to which the purposes of the project are compatible with those purposes.
- If information is to be obtained indirectly, explain why direct collection from the individual is not planned.
- Outline the proposed steps to make individuals aware of the project's purposes and use of the information.
- Outline what authorisation is relied upon to obtain information. For instance, with a public body this might be a provision in a particular law or it might be based on the agreement of the individual concerned.
- Are there special sensitivities about the information to be collected (for instance, racial origins or religious affiliations, information about children) or the means of collection (for instance, the use of biometrics, fingerprinting, video or audio-recording or the tracking of a person's location)?
- If a website is involved, are cookies transmitted or received? Is behaviour-specific information in cookies used? Is there a documented procedure concerning the type of information logged or cached about customers?
- Will unique identifiers be demanded, collected or otherwise involved in the collection process?
- Is information to be sourced from public registers? If so, consider the public register privacy principles as well as the IPPs.

Use, disclosure and retention of information

This will be an important part of any privacy impact report. The appropriate approach may vary considerably and the material below merely sets out typical matters to address. The nature of a particular project will dictate whether more or less attention needs to be paid to particular aspects of use, disclosure or retention.

- Describe all intended uses of personal information. Indicate the purpose of each. Explain whether the purposes are consistent with those for which the information was collected or obtained.
- In a similar way, describe and explain issues of disclosure.
- Which staff, classes of personnel, agents or contractors will have access to the information? For what purposes? How will the access or disclosure be controlled?
- How are individuals whose information is to be used or disclosed made aware of the purpose of that use or disclosure? Is their authority to be obtained? Are individuals permitted to opt out and if so how is that to be done?
- Does the use of the information involve any information matching procedure? If so, the privacy impact report will need to consider some special issues if public bodies are involved. The Office of the Privacy Commissioner can provide further guidance but the privacy impact report will, in particular, need to consider the information matching guidelines in section 98 of the Act.
- Are there special sensitivities about the uses? For instance, automated decision-making affecting individuals, surveillance or profiling. Might the uses lead to disciplinary action for individuals or some form of adverse outcome?
- Will personal information be transferred outside New Zealand? If so, outline aspects of the transfer including details of the receiving country. Explain steps to be taken to protect the information and the interests of the people concerned.
- If the Privacy Commissioner has issued a relevant code of practice, the privacy impact report should describe how the project will comply.
- What are the retention and destruction practices?
- Will unique identifiers or public register information be used?

D. PRIVACY RISK ASSESSMENT

The risks of the project can now be summarised and assessed. (Alternatively, the risk assessment may be integrated into the privacy analysis of the collection and obtaining of personal information and its use, disclosure and retention. There may nonetheless be value in briefly summarising the results and comparing the identified risks in a single place.)

The risks associated with failing to address the privacy implications of a given proposal can take many forms, and may include:

- failing to comply with either the letter or the spirit of the Act, or fair information practices generally, resulting in criticism from the public or Privacy Commissioner or complaints under the Act
- stimulating public outcry as a result of a perceived loss of privacy or a failure to meet expectations regarding the protection of personal information
- loss of credibility or public confidence when the public feels that a proposed project has not adequately considered or addressed privacy concerns
- underestimating privacy requirements with the result that systems need to be redesigned or retrofitted at considerable expense.

An important consideration is the expectations of the general public, customers, clients or employees. Proposals may be subject to public criticism even where the requirements of the Act have been met. If people perceive their privacy is seriously at risk, they are unlikely to be satisfied by a company which justifies its actions merely by pointing out that technically it has not breached the law.

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or obtaining sensitive details in unexpected circumstances all represent risks to the individual. Unexpected or unwelcome use or disclosure of that information, or its retention for an unduly long period, put privacy at risk. One task of the PIA is to sort out which risks are serious and which are trivial. The privacy impact report should identify the avoidable risks and suggest cost-effective measures to reduce them to an appropriate level.

Consider the following:

- How might individuals be affected by the risks identified?
- What is the likelihood of the risks? What is the range of possible adverse outcomes from least to most severe?
- Try to put yourself "in the shoes" of an affected person. How would an ordinary employee react if this scenario were to eventuate? Would a customer be surprised, or concerned, to see his or her details put to this use? If security were to be breached, or procedures not followed what might be the effect on individuals as a result?
- Do the public or customers have heightened sensitivities about the data in the proposed system?
- Will the information remain in New Zealand? If data were to be transferred outside New Zealand there are special sensitivities.
- How might the Privacy Commissioner, or relevant statutory bodies or regulators, view the risks in question?

The report should include:

- a description of specific privacy risks that have been identified
- an analysis of options considered to lessen or avoid those risks
- a list of any residual risks that cannot be resolved and an analysis of the possible implications of those risks in terms of the effects on individuals, public or stakeholder reaction and the project's success.

E. PRIVACY ENHANCING RESPONSES

Having identified any privacy risks associated with the proposal, what is to be done? Suitable responses can range from doing nothing, through to abandoning the project altogether. For most projects, the response is likely to be somewhere in the middle. There will typically be privacy risks associated with the proposal justifying a management or technical response. A range of privacy enhancing responses may be appropriate to the identified risks.

Security responses

One set of privacy enhancing responses will involve security safeguards appropriate to the sensitivity of the information and the particular data handling practices. IPP5 requires that all reasonable steps be taken to ensure that personal information held by an agency is protected against loss, unauthorised access, use, modification or disclosure, or other misuse. The security measures should respond to the risks as identified in the privacy impact report. The OECD has coined a "proportionality principle" in its guidelines on protection of information systems which states:

> Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of, and degree of reliance on, the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

Privacy impact assessment does not seek merely to identify the strongest information security. It seeks to identify the most appropriate levels of security. A privacy impact report should canvass the options available to address a particular privacy risk and provide supporting reasoning and information about any conclusions or recommendations on security safeguards.

Other privacy responses

Examining privacy enhancing responses to the identified risks does not simply involve a recitation of encryption levels, access controls and other security features. It should also address the information and management needs of the project. Does the business really need to know a particularly sensitive item of information or can it proceed without it? Are the organisation's interests best served by adding transaction data to its data warehouse or should it be erased when no longer needed? Should a particular use of information only proceed if a customer or employee opts-in rather than operating on an opt-out basis?

One significant question is often not asked at all: does the business need personal information about identifiable people to fulfil its purposes? There are now a range of technologies available which allow for financial transactions to be completed electronically on an anonymous basis (sometimes referred to as Privacy Enhancing Technologies or PETs).

As a starting point, the following points may be considered:

- Have security procedures for the collection, transmission, storage and disposal of personal information, and access, been documented? The PIA should give special attention to the security procedures relating to the areas that have been found to constitute a risk.
- Are privacy controls in place for the project? For instance, "need to know" policies and procedures for personal information access, physical security and access controls, IT security and access controls.
- Have technological tools and system design techniques been considered which may enhance both privacy and security (e.g. encryption, technologies of anonymity or pseudonymity, PETs)?
- Has there been an expert review of all the security risks and the reasonableness of countermeasures to secure the system against unauthorised or improper collection, access, modification, use, disclosure and disposal?
- Have staff been trained in requirements for protecting personal information and are they aware of policies regarding breaches of security or confidentiality? Are there plans for updated training as a result of the project under review?
- Are there authorisation controls defining which staff may add, change or delete information from records?
- Is the system designed so that access and changes to data can be audited by date and user identification? Does the system "footprint" inspection of records and provide an audit trail?
- Are user accounts, access rights and security authorisations controlled and recorded by an accountable systems or records management process?
- Are access rights only provided to users who actually require access for the stated purposes of collection or consistent purposes? Is user access to personal information limited to that required to discharge the assigned functions?
- Are the security measures commensurate with the sensitivity of the information recorded?
- Are there contingency plans and mechanisms in place to identify security breaches or disclosures of personal information in error? Are there mechanisms in place to notify security breaches to relevant parties to enable them to mitigate collateral risks?
- Are there adequate ongoing resources budgeted for security upgrades with performance indicators in systems maintenance plans?
- What steps are to be taken to make affected individuals aware of the project as it affects their information? Is this to be a one-off exercise or are there ongoing implications?
- Is the privacy impact report to be made widely available? Is there to be public or stakeholder consultation, building upon the report?

F. COMPLIANCE MECHANISMS

A PIA should also consider how the privacy risks of the project will continue to be appropriately controlled into the future. If an agency already has good privacy compliance processes in place it may be a simple matter of slotting this project into them. A pro-active business or government agency may, for example, have an effective Privacy Officer or privacy team and an existing business-wide programme of compliance audits. However, if there is no well developed existing structure in place for privacy management the privacy impact report should canvass the future privacy management of the project.

The privacy impact report remains relevant for the project as long as the fundamental assumptions upon which it was based remain unchanged. However, what happens if an important part of the system is redesigned after completion of the privacy impact report or if external circumstances, such as customer expectations, significantly change? Experience may also show that faith in a particular safeguard was misplaced. Can privacy be effectively protected if there is no response to such new information?

Systems design is a dynamic process. Change may be likely if a privacy impact report is completed before a project "goes live". However, the privacy impact report must be completed before this point if it is to be useful in project decision-making. It may be appropriate to produce an interim privacy impact report followed by a final report. Alternatively, a completed report may be followed by a revised privacy impact report. For relatively minor changes it may be sufficient to attach a small addendum, noting the relevant change and analysing the implications (if any), so that this may be read with the original privacy impact report.

Consider:

- Have arrangements been made for audit, compliance and enforcement mechanisms for the proposed project, including fulfilling the commitments made by management following adoption of the privacy impact report?
- Has a procedure been established to log and periodically review complaints and their resolution with a view to improving information management practices and standards?
- Does the business have a policy to require significant future changes to the system to be subject to PIA?

G. CONCLUSIONS

While the format of the summary will vary depending on the organisation's needs and the nature of the proposal. It might convey some of the following information:

- Description of the proposal including objectives, parties involved, timing and key milestones, resource requirements, benefits to the business or public, and pointers to more detailed information about the proposal.
- List of relevant privacy requirements including applicable law, business policies and codes of practice.
- The specific privacy risks.
- Options for addressing or mitigating those risks, along with the implications of principal options examined.
- Brief analysis of experience in other organisations, in New Zealand or elsewhere, which have addressed similar risks and whether their approaches were successful.
- Identification of any residual risks that cannot be addressed through the proposed options and, where possible, the likely implications of those residual risks in terms of public reaction, project success and other business interests;
- A proposed privacy communications strategy, where appropriate, so that stakeholders are effectively informed.

Appendices may be used to improve readability. For instance, a brief discussion or summary of an aspect of data processing may be sufficient in the body of the privacy impact report with fuller details in an appendix. A table summarising and comparing issues that have been dealt with in various places in the report could be brought together in a conclusion or appendix. The appendix also provides a place to attach or list relevant documentation that the assessor has taken into account.

10. Privacy Impact Assessment – The Pay-off

The cost of preparing a privacy impact report can be justified.

Building trust in electronic service delivery and maintaining competitive advantage

Demonstrating that privacy interests will be appropriately managed in a particular project offers a means of building and sustaining high levels of trust and confidence in e-commerce and e-government. If privacy practice and the protection of personal information are exemplary this will reflect favourably upon the organisation's reputation. It may also facilitate growth by reinforcing loyalty and expanding the customer base. The use of PIA in important projects demonstrates a seriousness about fair information practices.

Businesses who are able to sustain a high level of trust and confidence can differentiate themselves from their rivals. Differentiation not only adds value to brands and their position in the marketplace, but also offers a competitive advantage.

Pro-active approach to privacy risk management

Privacy risks certainly exist in relation to e-commerce and e-government. There is every indication that the litigation risk will escalate and with some businesses this will not originate in New Zealand but from customers overseas. On a business-to-business basis, affiliates and others dealing with New Zealand-based electronic traders will increasingly seek tangible proof of compliance with privacy policies and commitment to data protection principles. Preparation of a privacy impact report is part of a demonstration of this. An investment in a privacy impact report may be regarded as one strategy for managing privacy risk.

The human factor

Senior management need to provide clear leadership on privacy issues in the new electronic environments. This can be achieved by championing a culture that is respectful of customers and citizens and implements effective privacy policies. Employing PIA on significant systems is one such policy. Inadequate leadership in this area will result in an environment in which employee judgment calls will substitute for thoughtful policies and best practice procedures. PIA can help management to identify and minimise risks.

11. Appendices

A. THE INFORMATION PRIVACY PRINCIPLES

Principle 1: Purpose of collection of personal information

Personal information shall not be collected by any agency unless-

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) The collection of the information is necessary for that purpose.

Principle 2: Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,-

- (a) That the information is publicly available information; or
- (b) That the individual concerned authorises collection of the information from someone else; or
- (c) That non-compliance would not prejudice the interests of the individual concerned; or
- (d) That non-compliance is necessary-
  - (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  - (ii) For the enforcement of a law imposing a pecuniary penalty; or
  - (iii) For the protection of the public revenue; or
  - (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
- (e) That compliance would prejudice the purposes of the collection; or
- (f) That compliance is not reasonably practicable in the circumstances of the particular case: or
- (g) That the information-
  - (i) Will not be used in a form in which the individual concerned is identified; or
  - (ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

Principle 3: Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of -
   (a) The fact that the information is being collected; and
   (b) The purpose for which the information is being collected; and
   (c) The intended recipients of the information; and
   (d) The name and address of -
      (i) The agency that is collecting the information; and
      (ii) The agency that will hold the information; and
   (e) If the collection of the information is authorised or required by or under law -
      (i) The particular law by or under which the collection of the information is so authorised or required; and
      (ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and
   (f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and
   (g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds -
   (a) That non-compliance is authorised by the individual concerned; or
   (b) That non-compliance would not prejudice the interests of the individual concerned; or
   (c) That non-compliance is necessary -
      (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
      (ii) For the enforcement of a law imposing a pecuniary penalty; or
      (iii) For the protection of the public revenue; or
      (iv) For the conduct of proceedings before any court or tribunal being proceedings that have been commenced or are reasonably in contemplation); or
   (d) That compliance would prejudice the purposes of the collection; or
   (e) That compliance is not reasonably practicable in the circumstances of the particular case; or
   (f) That the information -
      (i) Will not be used in a form in which the individual concerned is identified; or
      (ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4: Manner of collection of personal information

Personal information shall not be collected by an agency-

(a) By unlawful means; or

(b) By means that, in the circumstances of the case, -

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5: Storage and security of personal information

An agency that holds personal information shall ensure -

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against -

(i) Loss; and

(ii) Access, use, modification or disclosure, except with the authority of the agency that holds the information; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6: Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled -

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts IV and V of this Act.

Principle 7: Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled -
   (a) To request correction of the information; and
   (b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8: Accuracy, etc., of personal information to be checked before use

An agency that holds information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9: Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10: Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,-

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned; or

(c) That non-compliance is necessary -

  (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

  (ii) For the enforcement of a law imposing a pecuniary penalty; or

  (iii) For the protection of the public revenue; or

  (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to-

  (i) Public health or public safety; or

  (ii) The life or health of the individual concerned or another individual; or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) That the information-

  (i) Is used in a form in which the individual concerned is not identified; or

  (ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

Principle 11: Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds -

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure is to the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or
(e) That non-compliance is necessary -
    (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, investigation, prosecution, and punishment of offences; or
    (ii) For the enforcement of the law imposing a pecuniary penalty; or
    (iii) For the protection of the public revenue; or
    (iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to-
    (i) Public health or public safety; or
    (ii) The life or health of the individual concerned or another individual; or
(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or
(h) That the information -
    (i) Is to be used in a form in which the individual concerned is not identified; or
    (ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Principle 12: Unique Identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.
(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those two agencies are associated persons within the meaning of section OD7 of the Income Tax Act 1994.
(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.
(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

B. BIBLIOGRAPHY

New Zealand materials

There are a number of books and other resources available on the Act and only a few are listed here. Current information can be obtained from the Privacy Commissioner's website and by contacting the privacy enquiries line.

- Privacy Commissioner's website: www.privacy.org.nz
- Privacy enquiries line: 0800 803 909
- Elizabeth Longworth and Tim McBride, *The Privacy Act: A Guide*, 1994
- Dr Paul Roth, *Privacy Law and Practice*, Butterworths, two volume loose-leaf service.

Published articles

The following articles each provides a slightly different perspective on PIA. Readers having difficulty locating the articles can obtain copies from the Office of the Privacy Commissioner.

- David Flaherty, "Privacy Impact Assessment: An essential tool for data protection", 7/5 *Privacy Law & Policy Reporter*, October 2000, 85.
- Blair Stewart (ed), "PIAs – An early warning system", 3/7 *Privacy Law & Policy Reporter*, November 1996, 134. This is an edited account of a conference panel session featuring Blair Stewart, Elizabeth Longworth, David Flaherty and Nigel Waters.
- Blair Stewart, "Privacy Impact Assessment: Towards a better informed process for evaluating privacy issues arising from new technologies", 5/8 *Privacy Law & Policy Reporter*, February 1999, 147.
- Blair Stewart, "Privacy Impact Assessment: Some approaches, issues and examples", in Hong Kong Privacy Commissioner for Personal Data, *E-Privacy in the New Economy: Conference Presentations*, March 2001, 67. This article listed more than 55 PIAs prepared between 1997 and 2001 in Hong Kong, Canada and New Zealand. A few are available on the Internet and many on request from the organisations concerned.
- Nigel Waters, "Privacy Impact Assessment – Traps for the unwary", 7/8 *Privacy Law & Policy Reporter*, February 2001, 161.
- Frank White, "The Use of Privacy Impact Assessments in Canada" 4/7-8 *Privacy Files*, 2001.

Other PIA guidelines

A number of models of PIA have been developed. The following, accessible on the Internet, may be of interest to anyone undertaking a PIA who seeks further guidance.

Deloitte & Touche, IT Governance Institute, Information Systems Audit and Control Foundation
A Guide to Cross-Border Privacy Impact Assessments, 2001
www.itgi.org/resources.htm

Internal Revenue Service, USA
IRS Privacy Impact Assessment, December 1996, endorsed by Federal Chief Information Officers Council in February 2000
www.cio.gov

Ministry of Management Services, British Columbia, Canada
Corporate Privacy Impact Assessment
www.mser.gov.bc.ca/foi_pop/manual/forms/pia.doc

Office of the Corporate Chief Strategist, Management Board Secretariat, Ontario, Canada
Privacy Impact Assessment Guidelines, June 2001
www.gov.on.ca/MBS/english/fip/pia/

Office of the Information and Privacy Commissioner, Alberta, Canada
Privacy Impact Assessment: Instructions and Annotated Questionnaire, January 2001
www.oipc.ab.ca

Office of the Information and Privacy Commissioner, British Columbia, Canada
Privacy Impact Assessment Model, December 1998
oipcbc.org/publications/pia

Office of the Privacy Commissioner, New Zealand
Guidance Note on Information Matching Privacy Impact Assessments, January 1999
www.privacy.org.nz

International materials

Information flows do not respect national boundaries – particularly in e-commerce. Accordingly, many PIAs will need to assess projects in the light of international standards and expectations and not simply New Zealand law. There is a vast international literature on data protection and information privacy. While no attempt is made to list materials here, anyone preparing a privacy impact report should consider the merit of undertaking a search of relevant literature. The principal international instruments on data protection and information privacy are:

- OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980
- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No 108), 28 January 1981
- United Nations General Assembly, Guidelines for the Regulation of Computerised Personal Data Files, 14 December 1990
- European Union, Directive on the Protection of Individuals with regard to the Processing of Personal data and on the Free Movement of such Data (95/46/EC), 24 October 1995.

In addition to these general international instruments there are a number of influential international guidelines on sectoral issues.

The Council of Europe and the institutions of the European Union have issued many guidelines and recommendations, too numerous to list here, which may be of assistance to anyone preparing a privacy impact report (refer **www.legal.coe.int/dataprotection/** and **europa.eu.int/comm/internal_market/en/dataprot/index.htm** respectively). In addition, regard may be had to the following:

- OECD, Guidelines for the Security of Information Systems, 26 November 1992
- International Labour Office, Code of Practice on the Protection of Workers' Personal Data, November 1996
- European Union, Directive on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (97/66/EC).

C. ACKNOWLEDGEMENTS

This handbook was written by Blair Stewart, Assistant Privacy Commissioner. In researching material for the handbook, several Canadians helpfully shared their experiences in the development of PIA guidelines, undertaking assessments and reviewing the results. Particular thanks are due to: Alec Campbell, former Director of Privacy Assessment, Office of the Information and Privacy Commissioner, Alberta; Guy Herriges, Management Board Secretariat, Government of Ontario; David Flaherty, Privacy and Information Policy Consultant, British Columbia. Helpful comment on drafts of the handbook were made by: Bob Stevens, Consultant in the Management of Personal Information and Privacy, Auckland; Wayne Wilson, Legal and Policy Adviser, and John Blakeley, Data Matching Compliance Officer, Office of the Privacy Commissioner, Wellington; Annabel Fordham, Executive Officer, Office of the Privacy Commissioner, Auckland. Margaret Gibbons typed the handbook. The handbook was initially prepared for the Office of the Privacy Commissioner for Personal Data, Hong Kong, as one of a series of "E-Privacy" handbooks. That office has kindly allowed the adaptation of the material for this New Zealand handbook.

ISBN 0-478-11703-5 – Handbook

PRIVACY IMPACT ASSESSMENT HANDBOOK

ISBN 0-478-11703-5 – Handbook

June 2007

Further copies available from the
Office of the Privacy Commissioner

Auckland office
P O Box 466, Auckland
Telephone 09-302 8680
Facsimile 09-302 2305
Email privacy@iprolink.co.nz

Wellington office
P O Box 10-094, Wellington
Telephone 04-474 7590
Facsimile 04-474 7595

Enquiries line
From Auckland: 302 8655
From outside Auckland: 0800 803 909

Internet
www.privacy.org.nz