

PRIVACY IMPACT ASSESSMENT: SOME APPROACHES, ISSUES AND EXAMPLES

Blair Stewart

Assistant Commissioner

Office of the Privacy Commissioner, New Zealand

ABSTRACT

The paper examines the concept and practice of privacy impact assessment (PIA). After introducing and defining the topic, the paper outlines some approaches (the “what”, “when”, “who” and “why” of PIA). The paper discusses aspects of the process from its start, where terms of reference are suggested, through its undertaking, with regard to a variety of guidelines, to the end of the process, where the PIA findings should be integrated into project decision-making. Following general coverage of the subject, the paper examines several particular issues including the relationship between PIA and privacy law, the role of lawyers, public access to PIA findings, and whether PIA should, in addition to identifying alternatives to a proposal, evaluate such alternatives. The paper closes with three appendices which set out recent articles, guidelines adopted in several jurisdictions and, for the first time, lists PIAs undertaken in Hong Kong, New Zealand and Canada.

this paper shows the practice of PIA has significantly gathered pace since 1999 as its merits have been identified and the preparation of such assessments has become mandatory in several jurisdictions.

This paper outlines some approaches to PIA and some current issues in the process. It also directs readers to a variety of resources that have become available in the last couple of years including a range of published papers and guidelines. For the first time a relatively comprehensive list of PIAs known to be in the process of preparation, or completed, in New Zealand, Canada and Hong Kong is set out. Although not all of those may yet be publicly available, it is anticipated that those PIAs will provide a valuable resource across all jurisdictions as to the issues under examination.

INTRODUCTION

The process of privacy impact assessment (PIA) is a valuable technique for identifying future privacy and data protection impacts and for reducing or mitigating any adverse effects. References to the potential of privacy impact assessment can be found at least as early as 1989¹ and official guidelines for the preparation of PIAs date from at least 1991.² However, as Appendix C to

¹ See David Flaherty, *Protecting Privacy in Surveillance Societies*, 1989, page 405.

² See State of New York Public Service Commission, “Statement of Policy on Privacy in Telecommunications”, 22 March

1991, reprinted in Information and Privacy Commissioner of Ontario submission to the Ontario Telephone Service Commission “Privacy and Telecommunications”, September 1992.

APPROACH TO PRIVACY IMPACT ASSESSMENT

Until recently there was little written on the subject of PIA. However, in the last two years, there have been several detailed papers published that go into many of the issues of definition and approach to privacy impact assessment³ and a range of guidelines for privacy impact assessments have become available.⁴ Accordingly, in this brief paper I do not intend to go into such matters in detail but merely touch on some issues of approach to undertaking privacy impact assessment.

What is privacy impact assessment?

Generally, the International Association for Impact Assessment defines impact assessment as “the identification of future consequences of a current or proposed action”.⁵ Consistent with that I have previously suggested the following definition:

“PIA is an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.”⁶

David Flaherty recently observed that:

³ The most complete recent treatment of the subject can be found in Waters (2001), Flaherty (2000) and Stewart (1999). A select bibliography is given at Appendix A.

⁴ Appendix B refers to four sets of Canadian guidelines that have been adopted in the last 2 years. Within these can also be found several templates for preparing PIAs.

⁵ <www.iaia.org>

⁶ Stewart, 1996a, 1999. In those papers I offered an alternative definition that “PIA is a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal.” As discussed further in the paper, there are some questions regarding the appropriateness of PIA identifying and evaluating alternatives to the basic proposal and for this reason I no longer favour this definition.

“Simply put, a privacy impact assessment seeks to set forth, in as much detail as required to promote necessary understanding, the essential components of any personal information system or any system that contains significant amounts of personal information.”⁷

That encapsulates guidance as to the amount of detail needed (sufficient “to promote necessary understanding”) and the features to concentrate on (“the essential components ...”). However, a PIA will often look beyond just a “system” *per se* into, for instance, “downstream” effects on persons who are affected in some way by the proposal.

PIA should properly be distinguished from privacy audits, privacy compliance audits or privacy risk assessments. Those other data protection techniques are applied to *existing* systems to ensure their continuing conformity with internal rules and external requirements. PIA, by contrast, focuses on understanding a *future* system with a view to identifying and mitigating forecast adverse impacts and informing decision making as to whether the project should proceed and in what form.

When might PIA appropriately be undertaken?

PIA may be desirable to assess risks:

- arising from a new technology or the convergence of existing technologies (for instance, electronic road pricing or other intelligent transportation system applications, person- location or person-tracking using cellphone or GPS technologies);
- where a known privacy-intrusive technology is to be used in new circumstances (for instance, expanding data matching or drug testing, installation of CCTV in public places);
- in a major endeavour or changing practice having significant privacy effects (for instance, a proposal to merge major public registries into a “super registry”, to adopt a national ID

⁷ Flaherty, 2000.

card, to confer state powers to access computer systems).

Appendix C illustrates where PIA has been seen as appropriate. PIA has been undertaken, for instance, in relation to:

- public health surveillance or database projects;
- interlinking of medical databases or providing access to electronic medical records;
- occupational or insurance surveillance projects involving the collation of adverse features or risk elements;
- creating, assigning and sharing unique identifiers within particular populations;
- applying new technology to personal identification documentation;
- installing recorded or real-time remote surveillance in public places;
- significantly expanding access to existing databases;
- establishing large data warehouses.

In the examples in New Zealand, Hong Kong and Canada the greatest use of PIA has been in relation to projects initiated by public authorities. However, the practice is also suitable for private sector initiatives and several examples initiated or affecting private sector bodies are included from the insurance and health area.

Are PIAs required to be prepared?

In several jurisdictions agencies can be required to complete a privacy impact assessment. For instance:

- In **Alberta** the Health Information Act 2000 requires that the Information and Privacy Commissioner be given a privacy impact assessment before a custodian implements “proposed administrative practices and information systems relating to the collection, use or disclosure of individual identifying health information”,⁸

⁸ Health Information Act (Alberta), section 64. There is also authority for privacy impact assessments under Alberta’s Freedom of Information and Protection of Privacy Act 1995, section 51(1)(f), in

- In **Ontario** it is a requirement of the Management Board Secretariat that a PIA be required where proposals and submissions “may affect client privacy”;⁹
- In **New Zealand** the Privacy Commissioner has required one agency to submit a privacy impact assessment when seeking an exemption by way of code of practice¹⁰ and also requires the submission of an information matching privacy impact assessment by departments proposing new authorised information matching programmes.¹¹

It appears likely that PIAs will increasingly be required of public bodies when developing significant new systems which will affect privacy. Perhaps PIA may also occasionally be required of private bodies. The requirements might be imposed in the following ways:

- new laws may directly oblige the preparation of PIAs or empower statutory officials to require them in appropriate cases;
- PIAs may be requested as part of approval or exemption processes;

relation to proposed legislative schemes or programmes of public bodies. While PIAs are recommended for major projects they are not mandatory under that Act.

⁹ Management Board Secretariat, PIA guidelines, pages 6 and 7. A process exists in Ontario for determining which projects require PIA involving annual Information and Information Technology plans and consultation between the sponsoring Ministries and MBS. Generally, minor changes to existing programmes do not require a PIA. New programmes that involve significant collection, use or disclosure of personal information need a PIA. Within the area of major changes to existing programmes there is discretion as to whether PIA is required (sometimes it will only be required for certain features of the proposed changes).

¹⁰ Ministry of Education Proposal to Develop a National Student Index Number.

¹¹ IMPIA guidelines and a list of IMPIAs is given in the appendix.

- corporate and governmental policies may anticipate completion of a PIA as a good practice requirement.

However, for the foreseeable future there will be no legal requirement to prepare PIAs for most agencies. Instead a decision to undertake privacy impact assessment will be based on the advantages of doing so. Other papers have canvassed the merits of privacy impact assessment thoroughly and I do not wish to repeat that material in any depth. Some of the advantages would include:

- as a tool to force the systematic analysis of privacy issues in order to inform debate on the proposal by decision-makers;
- a wish to understand the privacy pitfalls so as to avoid any adverse customer, employee or other stakeholder reaction to new systems;
- a kind of “early warning device” to save money and protect reputation - in some cases companies have met bitter consumer and public reaction which has led to the withdrawal of a new, and expensively developed, product for privacy reasons;¹²
- PIA brings responsibility clearly back to the proponent of a new proposal and implies that they must “own” and solve, or at least mitigate, the adverse privacy effects in their design and planning phases;
- desire for a cost-effective privacy impact mitigation since changes to meet privacy concerns, for instance by adopting privacy enhancing technologies, are cheaper at the design phase well before a system is operational;
- PIA reports can provide a credible source of information for proponents, regulators and the public - the PIA need not merely identify potential problems, it can allay concerns that

would fester if no credible or detailed analysis were to be available;

- PIA can be cost-effective also for privacy regulators who critique reports rather than undertaking field research themselves.

What goes into a PIA?

The guidelines listed in Appendix B go into considerable detail about the types of matters that will need to be gone into with a PIA.

David Flaherty has suggested a list of 26 items that could form a table of contents for a model privacy impact assessment and has summarised these to 7 broad headings:

- Introduction and overview;
- Description
- Data collection
- Disclosure and use of data
- Privacy standards and security measures
- Conclusion
- Sources.¹³

A typical list of matters that a PIA might describe in relation to a proposed scheme would include:

- the personal information in which the proposed scheme deals
- the sources from which this information is to be obtained
- the circumstances in which collection is to take place
- the processing (including collection or inter-connection) of that information
- the intended uses of the information held or thus produced
- the proposed recipients and their intended use of it
- the circumstances in which processing, use and disclosure is to take place
- the safeguards which will be operated against unauthorised access, use, disclosure, modification or loss.

Who prepares a PIA?

¹² Elizabeth Longworth has referred to the “front page test”: Will my company look bad in tomorrow’s newspaper when the public reacts to the information aspects of a new product? See Stewart, 1996b.

¹³ See Flaherty, 2000, pages 266-267 and footnote 4.

To be credible and effective:

- PIA should use competent expertise
- PIA should include an independent component.

What constitutes “**competent expertise**” will vary depending on the proposal being evaluated. A variety of skills are required which one individual may not possess and so a lead PIA coordinator may draw on the skills of others. The coordinator might be a generalist with perhaps other experts hired for their particular expertise. The initial PIA recently undertaken for the Hong Kong ID card project provides an example of a team approach, bringing international expertise together in several disciplines.¹⁴ In other cases, a single competent expert has undertaken PIA alone.¹⁵

For a PIA to be credible the other feature that is necessary is that there be some “**independent component**”. It would be difficult for Privacy Commissioners or the public to have complete confidence in a PIA which had been written solely by agency staff who are closely involved in driving a particular proposal notwithstanding the personal expertise and integrity of such people.

However, it is not necessarily the case that PIA must always be produced in a process that has absolute independence from the proponents of a project. That may not always be feasible. For example, it is almost inevitable the cost of undertaking PIA will be borne by the proponent. That of itself is not necessarily a problem. Typically a satisfactory degree of independence can be obtained by having the PIA undertaken by a paid professional who, while subject to some direction from the proponent as to such matters as timing, operates in an independent fashion. A

¹⁴ See Waters (2001), footnote 1.

¹⁵ For example, several of the Health Canada PIAs mentioned in Appendix B have been undertaken principally by the former Information and Privacy Commissioner of British Columbia.

consultant with appropriate privacy expertise will sufficiently value his or her continuing reputation as to offer objective and credible comment and recommendations.¹⁶ The consultant must indicate that the report constitutes his or her independent opinion – it is not given merely as the “mouthpiece” of the client.

A vexed issue in this context is whether it is possible for an organisation to prepare a *credible* PIA “in-house” within the organisation. I leave this as an open question. I certainly acknowledge the value of internally-produced analysis and reports on the kind of issues that might be turned over for external PIA. Certainly if an internal PIA is to be attempted it would be essential for it to be undertaken by staff who are not actively involved in the project itself. Someone who has been intimately involved in designing a proposed system, or whose continued employment or advancement is linked to the particular project, will be perceived to lack the objectivity and credibility needed to produce a PIA. In a large organisation it may be appropriate to draw on appropriate expertise in teams or offices unconnected with the project itself. There may, for instance, be a capacity to undertake PIA utilising the Chief Privacy Officer’s staff. In other cases, an independent element can be added to the process of internal PIA by external review. For instance, an external privacy expert might critique or review the document.¹⁷

¹⁶ A valuable discussion of some of the issues of independence are given in Waters, 2001, with the suggestion that ideally it would be desirable for the commissioning of PIAs to be done by someone other than the scheme proponent (although this will often not be possible). Waters discusses some of the contrary views and notes the need for proponents to develop a sense of “ownership” of the issues which may not be possible for an externally commissioned PIA.

¹⁷ For example, in Ontario and Alberta, PIAs are submitted to the Management Board Secretariat and the Information and Privacy Commissioner respectively.

What happens when the PIA is complete?

To be meaningful, the PIA has to be integrated into the decision-making process for the particular proposal. The value of a PIA is severely diminished if it is simply an afterthought once all decisions have been taken and a system is already in construction. Indeed, it is valuable to think of PIA as a *process* of assessment rather than solely focusing on the final complete document. Sometimes that process will be best achieved by a series of interim reports as general development of the proposal is refined. For example, in early stages of the design of a project an initial PIA might look broadly at the privacy issues and identify major risks with the various options under consideration. As the proposal firms up, the organisation may select one major alternative over another. At this point, a more detailed PIA might be developed which goes into all the various relevant issues.

Before the PIA is finally completed, it may be valuable to submit a draft version to appropriate privacy experts for peer review. For example, the Privacy Commissioner's office may be willing to comment on a draft PIA and the author may wish to refine any observations or conclusions based on that further input.

Once the PIA is finally completed it will be signed off by the principal author. This might be done in some agreed format to signify that the author has considered the issues raised by the proposal and that the report reflects his or her opinions as to the privacy risks and benefits. Insisting upon some kind of certificate like this may help ensure that the author associates his or her professional reputation with the conclusions. This seeks to address the risk that the PIA report be written simply to represent the client's views.

Typically a PIA will present a structured set of findings and possibly even recommendations. If recommendations are offered there should be a process

whereby they are evaluated and stakeholder and decision-maker responses are presented in a fashion that can be read with the PIA. The process associated with evaluation of the recent interim PIA for the Hong Kong identity card project offers a useful model as to how this might be done. Available on the LegCo website is a paper listing against each of the PIA recommendations the response from the Privacy Commissioner for Personal Data and the Government.¹⁸

SOME FURTHER ISSUES

The recent papers on PIA by David Flaherty and Nigel Waters offer a series of valuable insights into the challenges in effectively undertaking PIA. I encourage anyone contemplating undertaking or commissioning a PIA to study both articles. I now canvass some further issues not completely explored in those papers. I tentatively conclude that some of these, and some of the issues mentioned in those other articles, should be addressed upfront at the beginning of a PIA process through formal terms of reference.

What is the role of PIA in a jurisdiction which has a privacy law?

Over the last four or five years there has been lively international debate about various techniques and methods for effectively tackling privacy and data protection issues. Included amongst the discussion have been data protection law, self-regulatory initiatives, privacy enhancing technologies, international standards, sectoral v. omnibus rules and privacy impact assessment. There has been debate about which techniques are effective and whether they should be used in combination or alone.

Experience seems to suggest that PIA actually comes into its own in jurisdictions with privacy law. In those jurisdictions organisations are obliged to follow fair information practice but cannot always be

¹⁸ <www.legco.gov.hk/yr00-01/english/panels/se/papers/b752e04.pdf>

sure what is the right thing to do with complex new proposals. PIA provides the process to make better informed decisions that both respect privacy and comply with the law.

However, one risk of PIA in jurisdictions with privacy laws is that the process can be misunderstood and equated with a privacy compliance audit. This is a particular risk where PIA is undertaken by lawyers who concentrate solely on legal compliance rather than identifying and assessing privacy impacts. The PIA process should go beyond the legal tests in data protection law, which represent minimum acceptable practice, into identifying best practice and identifying the ways through mitigation, or identification of alternatives, a privacy-respectful outcome can be obtained.

It is open to decision-makers to disregard the findings of a PIA to instead favour a lower standard which nonetheless complies with the jurisdiction's law. However, in doing so the PIA will have informed the decision-makers as to the choice they are making. The PIA should not simply be a glorified legal opinion. If necessary, the proponent of a particular scheme should commission a legal opinion in tandem with commissioning a privacy impact assessment, or later, to fully inform the organisation about available legal options as well as preferred privacy options.

Must the completed PIA be made publicly available?

Whether or not a completed PIA *must* be made publicly available is a legal issue which would have to be determined in a particular case taking into account the laws of the particular jurisdiction. For instance, if a PIA is commissioned by a public body in a jurisdiction that has freedom of information (FOI) laws, the PIA will typically have to be made publicly available on request at some stage. On the other hand, if there is no FOI law, or the organisation commissioning the PIA is a private body to which no FOI law

applies, it is unlikely that the PIA must be made available.¹⁹

However, perhaps the more important question is whether the PIA *should* be made publicly available. In my view, if decision-makers decide to go ahead with a proposal after receiving a PIA, they ought to make the PIA publicly available or at least to the section of the public affected by the proposal.²⁰ It can be argued that one of the merits of a PIA should be to inform all those who will be affected by the proposal, not simply those who own the system.

If a private sector company examines a proposal but for privacy, or any other reasons, decides not to pursue that proposal that it might reasonably keep the completed PIA to itself.

Occasionally, PIAs will include material that is sensitive and which should not be released for reasons of public safety, maintenance of the law or to protect commercial secrets. All FOI laws contain procedures and withholding grounds to enable such material to be severed from the main report when releasing copies publicly.

Should PIAs identify and evaluate alternatives to the principal proposal?

A thorough PIA might examine not only the proposal at issue but also consider whether there is an alternative that is better from a privacy perspective.²¹

¹⁹ However, the PIA might be required to be disclosed to another body having powers to demand such documentation such as a legislative committee. Also if a private body shares a PIA with a public body, such as a privacy commissioner, it would usually become subject to FOI laws.

²⁰ For example, if only the members or employees of an organisation will be affected by a particular initiative it may be sufficient simply to circulate it to those people or make it available on request to that class of people.

²¹ For example, an assessment of a proposed data matching programme in New Zealand requires consideration of whether or not the use of an alternative means of achieving

However, that will not always be feasible or sensible. A lot depends upon the particular circumstances. For example, the only conceivable alternative to proposal A might be B. However, the team that has been put together to assess the effects of proposal A may have the wrong set of skills to examine B. Or it may be that B has already been ruled out for some other reason unconnected with privacy (such as cost or legality). It might also be a very expensive or time consuming process to adequately assess option B. Accordingly, in some cases it will be perfectly satisfactory to simply examine the privacy impacts of option A in isolation although the existence of B, as a theoretical possibility, would appropriately be noted.

On the other hand, it may well be appropriate to compare aspects of option A to B when, for example, trying to quantify and compare some benefit or cost of option A.

Furthermore, while at a macro-level it may be senseless in particular circumstances to digress to consider a full "option B", it may nonetheless be eminently sensible and appropriate – and indeed expected in a credible PIA – to examine micro-options to do with particular parts of a proposal. For example, in examining a proposal to place CCTV cameras throughout a public park it may not make sense to canvass an alternative of stationing a policeman in the park if the sponsoring organisation has no legal capacity to do so. However, the PIA would examine variations relating to the number of cameras, their siting, and examine their effectiveness and intrusiveness. It might even be that a micro-option, such as floodlighting a section of the park, might be examined as an alternative to the positioning of a CCTV camera in that section.

the objective of the programme would give similar significant and quantifiable monetary savings than the matching programme being examined. See Privacy Act 1993 (NZ) section 98(c).

No hard and fast rule can be made about the examination of alternatives but it will be a point of friction for any external reviewers, and the public, in considering the PIA if obvious alternatives are nowhere mentioned or examined. Sometimes the organisation commissioning the PIA should identify at the outset if there are aspects of the project that must be taken "as given" to avoid time being wasted on theoretical alternatives that the organisation cannot accept.

Establishing terms of reference

There may be value in formal terms of reference being established at the outset when a PIA is being commissioned.²² In doing so the credibility of the ultimate PIA must be given paramount consideration. If an organisation sidesteps the key issues through skewed terms of reference since it will remain ill informed after receiving the PIA and the public and any external body will be unimpressed with the assessment and react accordingly. That would be self-defeating.

However, in terms of the issues just mentioned, terms of reference might help assure that assessments:

- adequately deal with a range of privacy issues and do not simply focus on legal compliance;
- identify when the report is to be released publicly and in what fashion;
- identify whether or not major options are to be assessed.

It is suggested that if the PIA is ultimately to be reviewed by an external body that the terms of reference should be discussed with that body. The Privacy Commissioner may, for instance, be able to make suggestions as to important aspects to look at in the assessment.

²² This observation is less relevant in jurisdictions with detailed criteria as to what PIAs must cover such as Alberta and Ontario.

If formal terms of reference are to be established at the outset it makes sense for those to be peer reviewed by a person with suitable privacy expertise (possibly the person who will be undertaking the PIA itself). In some cases this will be the Privacy Commissioner, in other cases it might be a privacy consultant or the organisation's Chief Privacy Officer.

The terms of reference should contain sufficient flexibility for the author of the

PIA to delve into issues newly uncovered in the course of the assessment. The author of the PIA must have sufficient professional autonomy to undertake the task as he or she thinks fit. However, the terms of reference might indicate at least a minimum range of issues that must be assessed. They might also, as already discussed, limit the examination of certain alternatives where that is explicitly deemed necessary.

APPENDICES

A. SELECT BIBLIOGRAPHY

Roger Clarke's home page <www.anu.edu.au/people/Roger.Clarke/DV/PIA.html>

David Flaherty (2000), "Privacy Impact Assessments: An Essential Tool for Data Protection" in *One World One Privacy*, 22nd International Conference on Privacy and Personal Data Protection papers, September 2000, 77, revised version in *7/5 Privacy Law & Policy Reporter*, October 2000, 85 and Perrin, Black, Flaherty and Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, 2001, Appendix 5.

Privacy Laws & Business (2000), "Using Privacy Impact Assessments to Evaluate New Initiatives", *Privacy Laws & Business International Newsletter*, February 2000, 10.

Blair Stewart (1996a), "Privacy Impact Assessments", *3/4 Privacy Law & Policy Reporter*, July 1996, 61.

Blair Stewart (1996b), "PIAs – An Early Warning System", *3/7 Privacy Law & Policy Reporter*, October/November 1996, 134.

Blair Stewart (1999), "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.

Nigel Waters (2001), "Privacy Impact Assessment - Traps for the Unwary", *7/8 Privacy Law & Policy Reporter*, February 2001, 161.

B. PUBLISHED GUIDELINES FOR PRIVACY IMPACT ASSESSMENT

Responsible Organisation	Details of Guidelines
---------------------------------	------------------------------

Information & Privacy Commissioner, Ontario, Canada	Privacy Impact Assessment, Appendix A in <i>Geographic Information Systems</i> , April 1997 < www.ipc.on.ca >
Information & Privacy Office, Office of the Corporate Chief Strategist, Management	Privacy Impact Assessment Guidelines, May 2000 < www.gov.on.ca/MBS/english/fip/pia/ > Expected to be revised in June 2001.

Board Secretariat, Ontario,
Canada

Internal Revenue Service,
USA

IRS Privacy Impact Assessment, version 1.3, December 1996, endorsed by Federal Chief Information Officers Council in February 2000 <www.cio.gov>

Office of the Information and
Privacy Commissioner,
Alberta, Canada

Privacy Impact Assessment: Instructions and Annotated Questionnaire, Full Questionnaire and Supplementary Organisation Questionnaire, version 1.1, January 2001 <www.oipc.ab.ca>

Office of the Information and
Privacy Commissioner,
British Columbia, Canada

Privacy Impact Assessment Model, December 1998
<http://oipcbc.org/publications/pia>
See also <www.itsa.gov.bc.ca>

Office of the Privacy
Commissioner, New Zealand

Guidance Note for Departments seeking Legislative Provision for Information Matching: Information Matching Privacy Impact Assessments, revised version 20 January 1999 (available by email from privacy@iprolink.co.nz)

Treasury Board, Canada

Model Cross-Jurisdictional Privacy Impact Assessment Guide, Draft October 1999

C. EXAMPLES OF PRIVACY IMPACT ASSESSMENTS

These PIAs are not necessarily publicly available and any enquiries should be directed to the responsible organisation.

Responsible Organisation

Details of PIA

In preparation (as at 1 March 2001)

Management Board Secretariat,
Ontario, Canada

Ontario Government Smart Card Project

Ministry of Business Services,
Ontario, Canada

Registrar General – Registration Systems

Management Board Secretariat,
Ontario, Canada

Collection Management Unit Call Centre

Management Board Secretariat,
Ontario, Canada

Government of Ontario Public Key Infrastructure
Concept of Operations

Ministry of Business Services,
Ontario, Canada

Early Wins - Integrated Address Change Application

Management Board Secretariat,
Ontario, Canada

Federated Information Warehouse Model

Health Canada, Ottawa, Canada

Canadian Public Health Surveillance Project (CIPHS)

Health Canada, Ottawa, Canada

Product Related Toxicity Risk Data Network (ProdTox)

National Pilot System

Health Canada, Ottawa, Canada Spatial Public Health Information eXchange (Sphinx)

Land Transport Safety Authority,
Dunedin, New Zealand Proposed Operator Safety Rating System

Pharmacy Guild, Wellington, New
Zealand Primary Integration Network Project

Completed

Ministry of Education, Ontario,
Canada Elementary/Secondary Information System Data
Warehouse, February 2001

Ministry of Justice, Wellington,
New Zealand Justice Sector Code for Infringement Information,
January 2001 <www.privacy.org.nz>

Calgary Regional Health
Authority, Alberta, Canada Regional Staff Scheduling System, January 2001

Ministry of Education, Wellington,
New Zealand A proposal to develop a National Student Index
Number, December 2000

Immigration Department, Hong
Kong Hong Kong Identity Card Project – Initial Assessment,
November 2000

Ministry of Finance, Ontario,
Canada Integrated Financial Information System, October 2000

Ministry of Health, Ontario,
Canada Smart Card Health Initiatives Conceptual Design,
September 2000

Alberta Justice, Canada MEP Account Internet Access, September 2000

Alberta Health and Wellness,
Canada Collection of Treaty Status Flag Initiative, September
2000

Alberta Innovation and Science,
Canada IMAGIS Agent Project, August 2000

Alberta Health and Wellness,
Canada Pre-authorized Payment Plan, August 2000

Alberta Health and Wellness,
Canada Archival Blood Record Review Project, August 2000

Alberta Economic Development,
Canada Tourism Information System, August 2000

Management Board Secretariat,
Ontario, Canada Workforce Information Network Implementation, August
2000

Management Board Secretariat,
Ontario, Canada Directory and Messaging Project, August 2000

Health Funding Authority, Wellington New Zealand	Diabetes Disease Management in New Zealand, Primary Care Diabetes Management Component, August 2000
City of Quesnel, British Columbia, Canada	Installation of Video Surveillance in a Public Area, 2000
Alberta Alcohol and Drug Abuse Commission, Canada	AADAC System for Information and Service Tracking, July 2000
Alberta and Wellness, Canada	Interactive Voice Response (IVR) – Claims, Customer Service and Registration (CF&R) and Alberta Aids to Daily Living IVR Applications, July 2000
Aspen Regional Health Authority, Alberta, Canada	Teleultrasound, June 2000
Alberta Wellnet, Canada	Community-based Physicians Addendum to the Pharmaceutical Information Network's (PIN) Seniors Drug Profile, May 2000
Alberta Wellnet, Canada	Alberta Wellnet Spatial Public Health Information Exchange – Alberta Pilot Project (Sphinx-App), May 2000
Alberta Learning, Canada	National Student Number for the Enhanced Student Information System, April 2000
Alberta Provincial Mental Health Board, Canada	Telemental Health Service, April 2000
Alberta Wellnet, Canada	Non-Real Time Services Addendum, April 2000
Alberta Wellnet, Canada	Proposed Population Health Screening System, March 2000
Capital Health Authority, Alberta, Canada	Emergency Department Information System, January 2000
Calgary Regional Health Authority, Alberta, Canada	Teleradiology Initiative, December 1999
Alberta Wellnet, Canada	Tri-Regional Health Authority Administrative System, December 1999
Alberta Wellnet, Canada	Seniors Drug Profile Hospital/Medical Facility Expansion Addendum, December 1999
Capital Health Authority, Alberta, Canada	New Financial System, November 1999
Alberta Innovation and Science, Canada	IMAGIS Purchasing Policy, September 1999

Alberta Wellnet, Canada	Alberta Pilot Project (Sphinx-App), September 1999
Alberta Wellnet, Canada	TeleHealth Services (Remote Access to Health Services), August 1999
Ministry of Health, British Columbia, Canada	Wait List Registry, May 1999 < www.hlth.gov.bc.ca/waitlist/privacy.html >
Alberta Health, Canada	Communicable Disease Reporting System (STD Case Management Module, May 1999)
Alberta Mental Health Board, Canada	Alberta Regional Mental Health Information System, May 1999
Alberta Health, Canada	Rollout for the Pharmacy Information Network's Drug Profile System, March 1999
Alberta Economic Development, Canada	Clinical Information Systems of the Common Opportunities Project, March 1999
East Central Regional Health Authority, Alberta, Canada	MediPatient/MediPharm (Electronic Patient Records), March 1999
Alberta Health, Canada	Alberta Blue Cross MS Drug Coverage Initiative, March 1999
Health Funding Authority, Wellington, New Zealand	KidZnet Child Health Information Project, 1999
NZ Health Information Service, Wellington, New Zealand	Health Intranet Project, July 1998
Insurance Council, Wellington, New Zealand	National Fire and General Insurance Claims Register, June 1998
Land Transport Safety Authority, Wellington, New Zealand	Land Transport Rules: Driver Licensing (photo driver licence), November 1997

Additionally, a number of "Information Matching Privacy Impact Assessments" have been undertaken in New Zealand in relation to proposed government data matching programmes and submitted to the Office of the Privacy Commissioner. IMPIAs have been prepared in relation to the following data matching programmes:

- IRD/DWI Debtor Address Match
- Educational Institutions/DWI Loans & Allowances Match
- DWI/Courts Fines Defaulters Address Match
- IRD/Accident Insurance Regulator Employer Compliance Match
- IRD/Accident Insurance Regulator Sanction Assessment Match
- IRD/Courts Fines Defaulters Address Match
- ACC/IRD Child Tax Credit Match
- NZES/NZISS Match
- DWI/EEC Qualified Electors Match.

ACKNOWLEDGEMENTS

I am grateful to the following people for their help in collating the lists of guidelines for, and examples of, privacy impact assessments: Alex Campbell, Roger Clarke, Lorraine Dixon, David Flaherty, Guy Herriges, Nigel Waters. Comments by Bob Stevens and Wayne Wilson on a draft version of this paper were also appreciated.