Appendix C

Jurisdictional Report for Canada

CONTENTS

Terminology & Abbreviations

ATIP Access to Information and Privacy (Canada)

ARB Architectural Review Board (Ontario)

BC British Columbia, a province in Canada.

Central agency The agency within government that has overall responsibility for privacy policy. This agency may have some oversight responsibilities and usually has an advisory function.

DMIP Director/Manager of Information and Privacy (a mid-level managerial position in government ministries responsible for compliance with and operations relating to the *Freedom of Information and Privacy Act*). (BC)

EHR electronic health record (Ontario)

EIA Enterprise Information and Information Technology Architecture (Ontario)

EMR electronic medical record (Ontario)

FIPPA Freedom of Information & Protection of Privacy Act (Ontario)

HRDC Human Resources Development Canada, now Human Resources and Social Development Canada (HRSDC)

HRSDC Human Resources and Social Development Canada

I&IT Information and Information Technology (Ontario)

MFIPPA Municipal Freedom of Information & Protection of Privacy Act (Ontario)

MGS Ministry of Government Services (Ontario)

ON Ontario, a province in Canada

OSS Ontario Shared Services

Oversight body The organisation, usually independent of the administrative arm of government, with responsibility for monitoring compliance with privacy law. Very often the specific term used is a Data Protection or Privacy Commissioner.

At the federal level, this is the Office of the Privacy Commissioner. Provincially, this is the Office of the Information and Privacy Commissioner.

In ON, this is the Office of the Information and Privacy Commissioner, which fulfills a data commissioner function, with order-making authority.

OPC	Office of the Privacy Commissioner (Canada)
OIPC	Office of the Information and Privacy Commissioner (provinces)
PIA	Privacy Impact Assessment
PID	Personal Information Directory (BC)
PHIPA	Personal Health Information Protection Act (Ontario)
PIPEDA	Personal Information Protection and Electronic Documents Act
PIA	Privacy Impact Assessment
PIA-TRA	Privacy Impact Assessment - Threat Risk Assessment (Ontario)
PMFSC	Privacy Management Framework Steering Committee, Human Resources and Social Development Canada
PPIA	Preliminary Privacy Impact Assessment
Practitioner	Organisations or individuals who run programmes and enterprises and whose primary business is not privacy or data protection. Practitioners can be in the public or private sectors.
Privacy office	Internal department privacy staff, usually the ATIP office.
Regulators	The central agency and the oversight body, referred to collectively
TB	Treasury Board of Canada
TBS	Treasury Board Secretariat

I. CANADA, FEDERAL GOVERNMENT

Context

Canada is a federation composed of ten provinces (Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Quebec, and Saskatchewan), and three territories (the Northwest Territories, Nunavut, and the Yukon,). The population of Canada is roughly 32 and a half million.[1] Canada is a bilingual country, with both English and French as official languages at the federal level.

Canada is a constitutional monarchy with Elizabeth II, Queen of Canada, as head of state, and a parliamentary democracy with a federal system of parliamentary government. The basic framework of the Canadian constitution is contained in the Constitution Act 1867. It states that Canada has a constitution "similar in principle to that of the United Kingdom" and divides the powers between the federal and provincial governments. The Constitution includes the Canadian Charter of Rights and Freedoms, which guarantees basic rights and freedoms for Canadians.

The federal parliament is made up of the Queen and two houses: an elected House of Commons and an appointed Senate. The Queen is represented federally by the Governor General, and provincially by Lieutenant-Governors. The Canadian Prime Minister is appointed by the Governor General. All provinces have unicameral, elected legislatures, headed by a Premier. The national Parliament has power "to make laws for the peace, order and good government of Canada," except for "subjects assigned exclusively to the legislatures of the provinces." (Constitution Act 1897) This simple formulation disguises a complex national/provincial relationship as the Canadian courts have interpreted the powers granted to the provinces very widely. In addition, whilst the national Parliament and a provincial legislature cannot transfer any of their powers to each other, they can delegate the administration of their respective Acts to each other. The provinces are responsible for most of Canada's social programmes including health care, education, and welfare.[2]

In all the provinces, bar Quebec, there is a common law system. In Quebec there is a civil law system. Criminal law is solely a federal responsibility, and is uniform throughout Canada.

Legislative and Policy Framework

Legislation

Unlike the UK which has an overarching *Data Protection Act* which covers both public and private sectors, Canada has two federal privacy laws: the *Privacy Act*[3] and the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.[4] Oversight of both federal Acts is handled by the Privacy Commissioner of Canada (OPC) who is authorised to receive and investigate complaints.[5]

[1] Statistics Canada at: http://www40.statcan.ca/l01/cst01/demo02a.htm?sdi=population

[2] See further, http://www.parl.gc.ca/information/library/idb/forsey/PDFs/How_Canadians_Govern_Themselves-6ed.pdf

[3] Department of Justice Canada at: http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-21///en

[4] Department of Justice Canada at: http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-8.6///en

[5] Office of the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/index_e.asp

The *Privacy Act,* which came into effect in 1983, imposes obligations on specific federal government departments and agencies[6] to respect privacy rights by limiting the collection, use and disclosure of personal information. It gives individuals the right to access, and request correction of, personal information about themselves held by these federal government organisations.[7]

The President of the Treasury Board (TB) is the Minister responsible for government-wide administration of privacy legislation, under s.7 of the *Financial Administration Act* (Treasury Board Responsibilities and Powers) and para. 71(1)(d) of the *Privacy Act*. [8] The Treasury Board Secretariat (TBS), as the lead agency, co-operates with the Department of Justice in the area of legislative amendments and with the Privy Council Office regarding Cabinet confidences. The Secretariat also initiates and facilitates consultations with the OPC on policy matters. The TB issues directives and guidelines concerning the *Privacy Act* and its Regulations, and the Act is supported by a TB Privacy and Data Protection policy.[9] The objectives of that Policy are to:

- ensure the effective and consistent application of the provisions of the *Privacy Act* and the Privacy Regulations by government institutions;
- ensure data-matching and data linkage of personal information for administrative purposes meet the requirements of that legislation; and
- limit collection and use of the Social Insurance Number (SIN) for administrative purposes to those permitted by specific acts, regulations and programmes and to establish conditions for its collection.

Any personal information a federal department or agency that collects, uses and discloses must be registered with the Treasury Board Secretariat in a *Personal Information Bank* (PIB).[10] A statement of the purposes for which personal information in a PIB was obtained or compiled and a statement of the uses consistent with those purposes for which the information is used or disclosed must be included in the PIB description.[11] The PIB description is required to be published,[12] and can be found in *Info Source*, an annually updated TBS publication which identifies the content and location of Personal Information Banks.[13] The *Privacy Act* also requires that the head of every government institution prepares, for submission to Parliament, an annual report on the administration of the Act within the institution during each financial year.[14]

PIPEDA, which came into effect in stages from 2001, defines how private sector organisations may collect, use or disclose personal information in the course of commercial activities. The law gives individuals the right to access and request correction of the personal information these organisations may have collected about them. Matters of jurisdiction are complicated by the fact that:

[6] *Privacy Act,* Schedule: Government Institutions, Department of Justice Canada at: http://laws.justice.gc.ca/en/showdoc/cs/P-21/sc:1//en#anchorsc:1

[7] *Privacy Legislation in Canada*, Office of the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp

[8] *Privacy Impact Assessment Policy*, p.10.

[9] *Privacy and Data Protection Policy*, Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/dwnld/chap1_1_e.rtf

[10] s.10 *Privacy Act*.

[11] s.11(1)(a)(iv) *Privacy Act*.

[12] s.11 *Privacy Act*.

[13] *Info Source* at: http://infosource.gc.ca/index_e.asp

[14] s.72 *Privacy Act.*

The federal government may exempt [provincially regulated] organisations or activities in provinces that have their own privacy laws if they are substantially similar to the federal law. *PIPEDA* will continue to apply in those provinces to the federally regulated private sector and to personal information in inter-provincial and international transactions by all organisations engaged in commercial activities.

To date, British Columbia, Alberta and Quebec are the only provinces with laws recognised as substantially similar to *PIPEDA*.[15]

Table 1 – Canadian Provincial Private Sector Privacy Legislation

Province or Territory	Private Sector Legislation	Available at
Alberta	Personal Information Protection Act	http://www.pipa.gov.ab.ca/
British Columbia	Personal Information Protection Act	http://www.oipcbc.org/legislation.htm
Quebec	Protection of Personal Information in the Private Sector Act	http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html

At the provincial level, all the provinces and territories have privacy legislation governing the collection, use and disclosure of personal information held by public sector agencies (with varying levels of independence from government proper)[16], although that of Newfoundland and Labrador is not yet in force. These acts provide individuals with a general right to access and correct their personal information. Provincial oversight is via an independent commissioner or ombudsman authorised to receive and investigate complaints.

Table 2 - Canadian Provincial Public Sector Privacy Legislation

Province or Territory	Public Sector Legislation	Available at
Alberta	Freedom of Information & Protection of Privacy Act	http://foip.gov.ab.ca/legislation/index.cfm
British Columbia	Freedom of Information & Protection of Privacy Act	http://www.oipcbc.org/legislation.htm
Manitoba	Freedom of Information & Protection of Privacy Act	http://www.gov.mb.ca/chc/fippa/actandregs/index.html
New Brunswick	Protection of Personal Information Act	http://www.gnb.ca/0062/PDF-acts/p-19-1.pdf http://www.gnb.ca/0062/PDF-regs/2001-14.pdf
Newfoundland and Labrador	Access to Information and Protection of Privacy Act	http://www.hoa.gov.nl.ca/hoa/statutes/a01-1.htm
Northwest Territories	Access to Information and Protection of Privacy Act	http://www.justice.gov.nt.ca/pdf/ACTS/Access_to_Information.pdf
Nunavut	Access to Information and Protection of Privacy Act	http://action.attavik.ca/home/justice-gn/attach-en_conlaw_prediv/Type002.pdf

[15] *Substantially Similar Provincial Legislation*, Office of the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/legislation/ss_index_e.asp

[16] For instance, in some cases, self-governing professional bodies, local government bodies, health care delivery bodies and public utility corporations are covered.

Nova Scotia	Freedom of Information & Protection of Privacy Act.	http://www.gov.ns.ca/legislature/legc/statutes/freedom.htm
Ontario	Freedom of Information & Protection of Privacy Act	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
	Municipal Freedom of Information and Protection of Privacy Act	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm
Prince Edward Island	Freedom of Information & Protection of Privacy Act.	http://www.gov.pe.ca/law/statutes/pdf/f-15_01.pdf http://www.gov.pe.ca/law/regulations/pdf/F&15-01G.pdf
Quebec	Access to documents held by public bodies and the Protection of personal information Act	http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1_A.html
Saskatchewan	Freedom of Information & Protection of Privacy Act	http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf http://www.qp.gov.sk.ca/documents/English/Regulations/Regulations/F22-01R1.pdf
	Local Authority Freedom of Information and Protection of Privacy Act	http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/L27-1.pdf http://www.qp.gov.sk.ca/documents/English/Regulations/Regulations/L27-1R1.pdf
Yukon	Access to Information and Protection of Privacy Act	http://www.gov.yk.ca/legislation/acts/atipp.pdf

Additionally Alberta, Saskatchewan, Manitoba and Ontario have specific sectoral legislation dealing with the collection, use and disclosure of personal health information by health care providers and other health care organisations.

Table 3 - Canadian Provincial Health Information Privacy Legislation

Province or Territory	**Personal Health Legislation**	**Available at**
Alberta	Health Information Act	http://www.oipc.ab.ca/hia/act.cfm
Manitoba	Personal Health Information Act	http://www.gov.mb.ca/health/phia/index.html
Ontario	Health Information Protection Act	http://www.e-laws.gov.on.ca/html/source/regs/english/2007/elaws_src_regs_r07322_e.htm
Saskatchewan	Health Information Protection Act	http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf

At the federal level, Privacy Impact Assessments (PIAs) are not explicitly provided for in either the *Privacy Act* or *PIPEDA*. However, the federal policy on PIAs, discussed below, is premised on the basis that federal government departments and agencies should actively seek to be in compliance with the principles enumerated in the "Code of Fair Information Practices" in the federal *Privacy Act.*[17] PIAs are seen as an effective method

[17] Sections 4 to 8 of the *Privacy Act* deal with the collection, accuracy, use, disclosure, retention and disposal of personal information. They are based on the internationally accepted standards for the handling of personal information which are contained in the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" adopted

of achieving such compliance.[18] The federal PIA policy itself was issued by the Treasury Board of Canada (TB) under the powers described above.

Policy

A significant incident creating impetus for introduction of PIAs appears to have been 'the highly publicised debacle over Human Resources Development Canada's (HRDC) Longitudinal Labour Force File (LLF) whose … dismantlement, following public complaints about the database, cost the department millions of dollars.'[19] Concerns about the impact and cost of future privacy issues in the provision of government services led to Treasury Board being given the task of creating a PIA policy to act as a management tool to:

> ensure that privacy is considered throughout the design or re-design of programs or services. The assessments will identify the extent to which proposals comply with all appropriate statutes. Assessments [will] assist managers and decision-makers to avoid or mitigate privacy risks and promote fully informed policy, program and system design choices.[20]

The central agency responsible for government privacy policy is the Information and Privacy Policy office, Chief Information Officer Branch, Treasury Board of Canada, Secretariat (hereafter referred to as "the central agency") which administers and interprets the policy and which provides advice to institutions, the President of the Treasury Board and the Treasury Board. It is tasked with developing and maintaining guidelines to assist institutions in implementing the policy, and is also responsible for monitoring compliance.

The federal PIA policy applies to all government institutions listed in the Schedule to the *Privacy Act*, except the Bank of Canada. Departments and agencies are required to conduct and document PIAs for proposals for all new programmes and services that raise privacy issues.

If a proposal involves any of the following, a PIA is automatically required:

- A new or increased collection, use or disclosure of personal information, with or without the consent of individuals
- A broadening of target population
- A shift from direct to indirect collection of personal information
- An expansion of personal information collection for purposes of programme integration, programme administration or programme eligibility

by the Organization for Economic Co-operation and Development (OECD) accepted by Canada in 1984. Taken together, these sections of the Act constitute a "Code of Fair Information Practices". *Roles and Responsibilities*, Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_1-2_e.asp#leg This should not be confused with the CSA *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 that is embedded in PIPEDA and in the Ontario PHIPA.

[18] *Privacy Impact Assessment Policy*, p.1-4, Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piap-pefr_e.rtf

[19] *The Role of the Privacy Impact Assessment*, Stuart Bloomfield, (2004), Office of the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/speech/2004/sp-d_040310_e.asp *HRDC Dismantles Longitudinal Labour Force File Databank*, Human Resources and Social Development Canada at: http://www.hrsdc.gc.ca/en/cs/comm/news/2000/000529_e.shtml

[20] *Privacy Impact Assessment Policy*, p.2.

- New data matching or increased sharing of personal information between programmes or across institutions, jurisdictions or sectors
- Significant changes to the business process or systems affecting the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information
- Contracting out or devolution of a programme or service to other levels of government or the private sector
- Creation of a new or extended use of common personal identifiers
- An anticipated negative public response.

For programmes and services implemented prior to the PIA policy's implementation, institutions are required to undertake assessments where:

- services are substantially re-designed
- service delivery channels are substantially re-designed
- services are altered for electronic delivery in a manner that affects the collection, use or disclosure of personal information.

Departments and agencies are required to provide copies of their assessments to the Privacy Commissioner and publish summaries of the results in both official languages

The Canadian PIA Process

The central agency provides a considerable amount of information, including policy documents, guidance, and tools, the majority of which are readily accessible via its website. As of Summer 2007, the Office of the Privacy Commissioner of Canada (the oversight body) has been working on an Audit Report reviewing the federal PIA process. It seems likely that this Report will result in some revisions to the federal PIA process, tool and guidance material. At the time of writing, the Audit Report is not publicly available, as it has not yet been laid before Parliament. The following describes the current, information, process and tools which have been in place since May 2002.

Table 4 – Canadian central agency PIA policy, guidance and templates

	Purpose	**Available at**
PIA Policy (05/2002)	Sets out policy requirements, roles and accountability, monitoring and oversight.	http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piap-pefr_e.rtf
PIA Guidelines (08/2002)	Framework for the completion of a PIA, including: checklist for when a PIA is required; goals of a PIA; process overview (Resource Requirements, Documenting Data Flows, Privacy Analysis, Privacy Impact Analysis Report, Addressing Risks); questionnaire for federal programmes and services; questionnaire for cross-jurisdictional programme and service delivery; model table of contents for PPIAs and PIAs.	http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piapg-pefrld_e.rtf
PIA Report Template (08/2002)	Electronic template for standardised production of PPIAs and PIAs	http://www.tbs-sct.gc.ca/pgol-pged/ppia-epfvp/prelim-temp-modl/prelim-temp-modl00_e.asp
Report on PIA Best Practices (03/2003)	Identifies practical tips and best practices for implementing the *PIA Policy* and *Guidelines* into departmental day-to-day operations.	http://www.tbs-sct.gc.ca/pgol-pged/pia-best/pia-best00_e.asp

PIA e-learning tool (10/2003)	Overview module - a basic review of the basic principles of privacy in Canada and discusses the fundamentals of PIA process. Includes key privacy definitions, review of Canadian privacy legislation and policy, information about the main features and benefits of PIAs and an overview of the PIA process and the key stakeholders involved in PIAs.	http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a_e.asp
	Manage/Monitor module - reviews key concepts related to PIAs - the legislation and policy and the key stakeholders, but in less detail than Overview module Reviews the entire PIA process, including tips and techniques taken from the 'best practices' of Government of Canada (GoC) personnel involved in PIA projects – Aid to managing, co-ordinating and monitoring a PIA project	http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-b_e.asp
	PIA Assistant - Provides a step-by step 'walk through' of the PPIA/PIA process, e.g. how to write the Report's Executive Summary or how to use the Document Change Control Table, as well as completing the questionnaire for federal programmes and services or the questionnaire for cross-jurisdictional programme and service delivery. Provides links to items such as the *Privacy Act*, *PIPEDA* and even definitions of key terminology.	http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-c_e.asp
Privacy Impact Assessment Audit Guide (05/2004)	Presents the policy requirements, along with related information and key sources for understanding the basics of the PIA process; provides background information to broaden the reader's understanding of the responsibilities of key stakeholders involved in completing, reviewing and approving PIAs; and proposes audit objectives and criteria so that Internal Auditors may develop a customised audit programme using a risk based audit approach.	http://www.tbs-sct.gc.ca/ia-vi/policies-politiques/pia-efvp/pia-efvp_e.pd f

The PIA Tools

As noted in Table 4, the central agency publishes three standard tools for the conduct of PIAs:

1. The PIA Policy
2. The PIA Guidelines
3. The PIA Report Template

The Guidelines contain two compliance questionnaires, one for federal programmes and services, which provides a series of questions derived from the requirements of the *Privacy Act* (with questions linked to particular sections of the Act, as appropriate); and one for cross-jurisdictional programme and service delivery, which provides a series of questions derived from the universal privacy principles in the Canadian Standards Association Model Code for the Protection of Personal Information. The yes/no/not applicable answers are augmented throughout the form with space for explanations.

The PIA Report template contains the following key elements:

- Executive Summary – this may be used to communicate the results of the PIA with the public

- Introduction – includes the PIA Report Objectives; a statement of work to be performed and any assumptions affecting the scope of work; reference documentation; list of participants contributing to the PIA; legislation and policies considered as part of the PIA.
- Project proposal – a narrative description of the project proposal including objectives, rationale, clients, approach and programmes and/or partners involved.
- Data flow analysis – including a flowchart and description to portray the major components of the business process; a data flow table to follow each data element or cluster from data collection through use and disclosure
- The appropriate questionnaire – No specific instructions are given for determining which questionnaire should be used, presumably because it was thought self-evident whether a programme or service would be federal or cross-jurisdiction. Given the increasing move towards Shared Services in the Canadian public sector, this might now seem to be an oversight.
- A privacy risk management plan – including a description of privacy risks and mitigation measures; a list of residual risks that cannot be resolved by means of the proposed options and an analysis of possible implications of these risks in terms of public reaction and programme success
- A communications strategy, as appropriate.

The PIA process overview describes the PIA as follows.

> Privacy Impact Assessments provide a framework to ensure that privacy is considered throughout the design or re-design of programs or services. The assessments will identify the extent to which proposals comply with all appropriate statutes. Assessments assist managers and decision-makers to avoid or mitigate privacy risks and promote fully informed policy, program and system design choices.[21]

This is expanded upon in the TBS PIA e-learning tool:

> [A PIA is a comprehensive process] designed to assist institutions in determining the effects of program and service delivery initiatives on individual privacy. The process is very similar to a continuous risk management approach in that it includes the following primary stages.
>
> - Project Initiation
> - Data Analysis
> - Privacy Analysis
> - Privacy Impact Assessment Report
>
> […]
>
> …the PIA process is a due diligence exercise where institutions can identify and address potential privacy risks that may occur in the course of their operations.
>
> […]
>
> The assessment process is iterative, meaning that it is to be updated, maintained, re-designed or altered throughout the life cycle of a program or service.

[21] *Privacy Impact Assessment Policy*, p.2.

The PIA process is supported by the web-based PIA e-learning tool which provides significant guidance to those undertaking PIAs. This provides a useful starting point for programme personnel to get to grips with PIA terminology and definitions. Education and training is seen as a key component of successful integration of PIA processes into departmental and project workflows, although a common refrain was that the acid test for understanding of the PIA process was to actually have conducted one.

<u>Completion of PIAs</u>

<u>By Whom?</u>

In principle, the completion and maintenance of PPIAs and PIAs is a

> shared management responsibility that requires the co-operation and support of various officials throughout institutions. Program and project managers, privacy policy and legal advisors and functional specialists must be involved to ensure that privacy implications are identified, assessed, avoided or resolved. Collaboration with communications staff is required to facilitate the timely dissemination of information to the public.[22]

In practice, it appears that departments and agencies handle completion of PIAs in a variety of ways, ranging from a relatively heavily structured internal process, involving project managers, privacy office staff,[23] legal officers, IT staff, Records Management staff, and as necessary private consultants; to the effective outsourcing of the PIA process to consultants. The OPC has encouraged departments to establish a formal administrative structure such as an internal committee or working group that is specifically responsible for reviewing departmental initiatives to determine whether they require a PIA, and for implementing privacy risk reduction measures after a PIA has been done.[24]

<u>When?</u>

Departments and agencies must initiate a PPIA or a PIA in the early stages of the design or re-design of a programme or service, so the results of the assessment can have the opportunity to influence the developmental process.

Preliminary PIA (PPIA)

A PPIA would likely be completed during the Project Initiation/Needs Assessment stage of a programme or service. The main reason for a department/agency choosing to conduct a Preliminary PIA instead of a full PIA will be that a proposal is at an early design stage and as a result, the department/agency lacks sufficient information to conduct a full PIA. As a PIA is a continuous process requiring updating to reflect programme, service or system changes, the results of a Preliminary PIA should facilitate the development of a full PIA. The Preliminary PIA will not be as

[22] *Privacy Impact Assessment Policy*, p.9.

[23] The privacy office in Canadian federal government departments and agencies is usually termed the Access to Information and Privacy (ATIP) office. *Access to Information and Privacy Coordinators*, Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/atip-aiprp/apps/coords/index_e.asp

[24] *Annual Report to Parliament 2005-2006 Report on the Privacy Act*, p.59. Office of the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.pdf

comprehensive as the PIA but will serve to indicate to departmental programme managers whether or not there are significant privacy risks for a proposal.[25]

Conducting a PPIA typically involves an assessment of the following:

- Identifying the types and volumes of personal information to be collected, used and disclosed.
- Verifying legislative and policy authorities for the proposed programme or service.
- Clarifying the roles, responsibilities and legal and policy status of the key stakeholders, including other jurisdictions and the private sector.
- Determining which aspects of the programme or service are likely to involve privacy risks.
- Initiating the consultation process with the Office of the Privacy Commissioner (OPC).
- Defining the scope and the schedule for the final assessment.

In *exceptional circumstances*, a Preliminary PIA can also be conducted if there appears to be uncertainty whether the proposal involves privacy issues.

Anecdotally, it appears that for some projects depending on size and scope, engaging in a preliminary PIA will take nearly as much time and resource as engaging in a full PIA.

External Consultation

While external consultation in the sense of consultation with the general public is encouraged, it is not mandatory, and the extent to which it takes place in many departments/agencies appears limited. Some departments/agencies have reported engaging in public consultation, but it is unclear what that consultation has entailed, and the extent of public consultation has not been formally reviewed. Most consultation that takes place is internal, although departments/agencies may consult with the OPC, other provincial and federal departments/agencies, private consultants, and private contractors who will be providing or facilitating services. The TBS has had requests for a generic PIA Report template in circumstances where departments are introducing similar systems. A generic PIA template for a specific area has been drafted by TBS that could be tailored to the needs of particular departments (not yet approved).

Review/Approval of PIAs

Internal

In broad terms a Canadian federal government department is headed by a Minister, which is a political position usually held by an MP who is a member of the Cabinet. The senior civil servant in a department is the Deputy Minister (or Deputy Head). They are responsible for the working of the department and report directly the Minister. Under the Deputy Minister, are a number of Assistant Deputy Ministers who oversee various broad aspects of the department (e.g. policy, administration, programme implementation). Below each Assistant Deputy Minister are a number of Director-Generals who oversee more functional areas of

[25] *Privacy Impact Assessment Guidelines*, p.6. Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piapg-pefrld_e.rtf

each broad element of the department. Under Director-Generals are Directors, who oversee various Directorates which are the core of any department.

There does not appear to be consistency in the internal review and approval process for PIAs as practiced by different departments and agencies. While Ministers for departments and other heads of institutions are responsible for ensuring that their institutions comply with the *Privacy Act*, Regulations and associated policies, it is Deputy Ministers and other deputy heads of institutions who are responsible for:

- promoting an awareness of PIA requirements within their institutions;
- determining whether initiatives have a potential impact on the privacy of Canadians and warrant the development of PIAs;
- integrating and balancing privacy with other legislative and policy requirements;
- ensuring that the process and tools used in assessing privacy impacts are as rigorous as those outlined in the PIA Guidelines;
- consulting with the Office of the Privacy Commissioner;
- approving the final PIAs to be provided to the Commissioner;
- responding to any advice that might be offered by the Commissioner;
- ensuring that PIA summaries are made available to the public.

As such PIAs must be signed off by Deputy Ministers or other deputy heads of institutions, but beyond that it appears that practice varies. If a PIA is not required, TBS suggests as a matter of good policy that sign-off' on that decision should be obtained to illustrate 'due diligence' and demonstrate that consideration was given to the idea, however, this is not mandatory.

Human Resources and Social Development Canada (HRSDC), which is divided into 11 major Branches, applies a rigorous internal review process that is often cited as an example of good practice. PIAs are carried out by Departmental staff in a particular Branch/region, sometimes with the help of external consultants. Their assessment has to be approved by the responsible Assistant Deputy Minister.

Completed PIAs are then presented by the branch to the Department's Privacy Management Framework Steering Committee (PMFSC) for review as the committee is responsible for recommending Deputy Minister approval of PIAs. The Privacy Management Framework Steering Committee (PMFSC) directs the development and implementation of the HRSDC Privacy Management Framework, which defines responsibility and accountability on privacy from the Deputy Minister to employees and across programmes. The PMFSC is also mandated to oversee the responses to corporate privacy policy issues.[26] PMFSC

[26] *Report: Audit of Management of Personal Information*, Human Resources and Social Development Canada at: http://www.hrsdc.gc.ca/en/cs/fas/iarms/sp-603-07-04e.shtml

The Privacy Management Framework is an overarching infrastructure to manage personal information within HRSDC. It is a framework of policies, guidelines, best practices and tools, including Privacy Impact Assessments and the work of the Databank Review Committee, whose objective is to examine administrative and research uses of personal information to assure that all privacy issues are identified and either resolved or mitigated.

convenes monthly and is composed of Director General-level participants from both Human Resources and Social Development Canada (HRSDC) and Service Canada (ServCan), along with representatives from three regions. When approval is obtained from the PMFSC, an approval package is sent to the Deputy Minister with recommendations of PMFSC.

Central Agency Review

Institutions seeking Preliminary Project Approval (PPA)[27] from Treasury Board under the Board's Project Approval Policy[28] must include the results of the Privacy Impact Assessment in the body of the submission or in the project brief. Institutions seeking Effective Project Approval (EPA)[29] from the Board must provide a status report in the body of the submission or the project brief summarising the actions taken or to be taken to avoid or mitigate the privacy risks, if any, as per the Privacy Impact Assessment. There is no specific review of the PIA, but the need for a PIA Report, and whether one has been conducted will be considered as part of the submission or project brief. Where a PIA has not been conducted and the TBS feels that one should, they may require the institution to undertake one, and may advise on specific issues that should be examined e.g. cross jurisdictional, transborder data flows.

Treasury Board approval of PPAs and EPAs takes the form of a decision letter. The department is accountable to the Board for meeting the objectives and any other directions, including privacy recommendations, set out in the decision letter.

The departmental Annual Reports to Parliament required by the *Privacy Act* s.72, which include details of PIAs undertaken during the year, are also forwarded to TBS. Additionally, TBS analysts are assigned to each institution and they may request that a PIA be completed. These analysts may also become part of the PIA Team and assist in the completion of a PIA.

Oversight Office Review

Treasury Board PIA policy requires that PIAs be shared with the Office of the Privacy Commissioner (OPC) to afford the Privacy Commissioner the opportunity to provide comments. The OPC's role is not to approve/reject submitted PIAs, but to comment on the quality of the process undertaken. In principle, this step could be satisfied by submission to the OPC, even where the OPC did not comment on a PIA. In practice, the OPC endeavours to comment on all PIAs submitted by departments and agencies. The OPC's Audit and Review group undertakes the reviews. The OPC will respond privately to the department or agency concerned about the PIA's quality. The department or agency may still

The Privacy Management Framework aims to demonstrate that current HRSDC and ServCan management of personal information is sound, and addresses the ongoing development of new programs and the redevelopment of existing ones.

[27] Departments normally request Preliminary Program Approval when the initial project planning and identification phase is completed but before the project definition phase starts. PPA provides authorisation to expend resources to fully define the selected project option.

[28] *Project Approval Policy*, Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/common/instruction_e.asp

[29] Departments submit for EPA before starting the project implementation phase. For those projects where the Treasury Board has not provided a PPA, the EPA must include all information required for PPA.

press ahead with the project, and the OPC may comment publicly on projects that appear to her to be problematic. In principle, reviews are to be carried out within approximately 6 weeks of submission.

There have been problems with the review process inasmuch as the OPC was under-resourced to deal with the number of PIAs it was receiving. This had led, by 2005-2006, to significant backlog of PPIAs and PIAs awaiting review, and a time delay in handling reviews.

> During 2005-2006 we received a total of 41 Privacy Impact Assessments (PIA) and Preliminary Privacy Impact Assessments (PPIA), and completed 43 PIA reviews. At the end of the year, there were 55 PIA or PPIA on hand, a reduction of 2 from the previous year. Because of inadequate resources in 2005-2006 and prior years a backlog has developed which has resulted in a lag of 6 to 9 months between the receipt of a PIA or PPIA from a federal department or agency and the start of our review.[30]

Additional resourcing/staffing has seen both the backlog and timelag decrease through 2007. However, it appears that the number of PIAs submitted for review is on the increase, as departments and agencies become more attuned to the privacy implications of their work, and privacy risk assessment becomes increasingly embedded in routine project management processes. It is worth reiterating that OPC review is not an authorisation process, and that projects can, and will, go ahead without an oversight office review having been completed.

Those undertaking PPIAs and PIAs are advised to seek advice from the OPC in the Treasury Board policy, and some departments and agencies do so before and during the undertaking of PIAs. Consultation may be directly sought by the person undertaking the PIA or filtered through their privacy office or co-ordinator. Despite this, the OPC frequently receives PPIAs and PIAs which do not contain enough information for the OPC to undertake a satisfactory review, for example a PIA might identify a privacy risk, but fail to provide an action plan to demonstrate how the department intends to address that risk.[31]

The OPC does not regard its review process as providing approval and, even in the event that there are no recommendations made about the PIA, or if the recommendations that are made are followed by the submitting department or agency, it reserves the right to comment on the programme or system in future and its input does not guarantee favourable rulings, should a case ever arise regarding the subject of the PIA. The review process will consider whether the new programme or system will comply with the law, but may also provide ideas about how programme goals could be achieved in less privacy invasive ways.

External Review

PIAs are not subject to external review.

[30] Departmental Performance Report for the fiscal year ending March 31, 2006, Office of the Privacy Commissioner of Canada, p.18. Treasury Board of Canada at: http://www.tbs-sct.gc.ca/dpr-rmr/0506/PCC-CPVPC/pcc-cpvpc_e.pdf

[31] Annual Report to Parliament 2005-2006 Report on the Privacy Act, p.56. Office of the Privacy Commissioner of Canada at: http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.pdf

Public Availability

Departments and agencies are required to make summaries of the results of their Privacy Impact Assessments available to the public. Publication has to be in a timely manner, using plain language, and in each of the two official languages. Departments and agencies are required to take into account, when publishing summaries, that PIAs could contain:

- elements should be protected under the *Access to Information Act* or the *Privacy Act*, and
- information that would render systems or security measures vulnerable, or refer to programmes or services that have not been formally approved or announced.

It is recommended by the TBS that both the Internet and conventional publishing should be used to disseminate assessments and may include references and links to related documentation.[32]

In practice, it appears that public availability of PIA summaries is limited, and that few departments and agencies are in total compliance, having failed to publish a complete set of summaries, failed to make summaries publically accessible by the Internet, or failed to publish PIA summaries at all. When PIAs are published, their quality is highly variable – while the Treasury Board policy suggests publishing the PIA Executive Summary from the formal PIA Report as the public summary, this rarely appears to occur, and some summaries are effectively limited to project descriptions and an assertion that privacy requirements have been identified and addressed.[33] There is currently no centralised mechanism for accessing summaries produced by federal government departments and agencies.

Lessons Learned

The nature of the PIA process, with early consideration of the privacy implications of new developments, often means that it can be difficult to identify in a completed PIA Report the extent to which the project, programme or service has been influenced by the assessment.

Participants in the TBS's Report on PIA Best Practices identified a number of benefits to departments associated with the PIA process:

- The PIA process makes project planners articulate in precise terms what the project is about.
- Privacy is considered at the front end of a project so that privacy issues are known and can be addressed early in the project planning process.
- The PIA process presents an opportunity to communicate, discuss and increase the awareness of the *Privacy Act*.
- The PIA process enhances programme planning relative to privacy and results in better public policy.

[32] *Privacy Impact Assessment Policy*, p.8.

[33] *PIA Summary: The Agency Data Warehouse (ADW)*, Canada Revenue Agency at: http://www.cra-arc.gc.ca/agency/privacy/pia/adw-e.htm
PIA Summary: High-Risk Traveller Identification Initiative, Canada Border Services Agency (CBSA) at: http://www.cbsa-asfc.gc.ca/general/pia-efvp/hrti_ivre_20051003-e.html

- The PIA process provides a disciplined approach to the identification and mitigation of privacy risks resulting in better information management practices.
- The PIA process is an excellent means to learn about privacy.
- Some departments reported a better understanding of the relationship between Program legislation and the *Privacy Act*.

PIAs have clearly made a significant difference in a number of cases. Three examples where a PIA has resulted in changes to an envisaged project, programme or service are:

- The Secure Channel Project. Secure Channel (SC) is at the centre of the Government of Canada's common secure infrastructure and the foundation of Canada's Government On-Line (GOL) initiative. SC provides citizens and businesses with secure and private access to all federal government on-line services. Part of the SC process involves using an 'epass', which is a unique electronic credential that allows individuals to communicate securely with online enabled Government services. During the Epass programme implementation there were a total of four iterative PIAs completed, as "the design of the programme, the architecture and specifications, and consequently the data-flows, continued to evolve over the course of several months."[34] The PIAs led to a number of changes to the project, which has been praised by the Privacy Commissioner for "…the creative approach … taken in addressing many of the privacy risks associated with more conventional on-line client authentication models."
- The Immigration – Contribution Accountability Measurement System (iCAMS). iCAMS is an Internet-based data collection system for settlement and resettlement contribution programmes used by Citizenship and Immigration Canada to gather information about clients and the services they receive. The PIA process for ICAMs resulted in a reduction in the amount of personal information that was to be collected, and a rethink of the processes surrounding the collection and use of the data.
- Human Resources Management System (HRMS) at Veterans Affairs Canada (VAC). A PIA was conducted to evaluate the Government of Canada Human Resources Management System (HRMS) as implemented by Veterans Affairs Canada. The PIA Report identified three areas of non-compliance with privacy requirements: safeguarding personal information (high-level risk), accountability and performance measures (high-level risk), and procedures and documentation (medium-level risk). Mitigating strategies were adopted for all three areas.[35]

The TBS PIA e-learning tool has not been actively updated since going live in 2004, While it is primarily a tool to create awareness of PIAs and to provide an overview of legal and policy privacy requirements, it contains elements which walk users through the PIA basics and, once users start working on a PIA it contains explanations about the nature and scope of the questions being asked in the Guidelines. In short, it appears to be considered by both BS, OPC and practitioners as a useful tool, which has been implemented, and can be maintained, at relatively low cost.

[34] Government of Canada's Legal and Policy Framework for Government On-Line, Treasury Board of Canada at: http://www.tbs-sct.gc.ca/pki-icp/gocpki/frame/frame05_e.asp

[35] *Privacy Impact Assessment of the Human Resources Management System for Veterans Affairs Canada*, at: http://www.gchrms.gc.ca/GCHRMSCluster/GCHRMSProducts/FunctionalDocumentation-Version%20Control/PIA/PIA.zip

The federal government PIA process in Canada is currently entering a review phase with both the OPC and the TBS examining the progress to date. As will be seen in the following section, both OPC and TBS feel that the process is still maturing, and that there remains scope for improvement in the policy process and implementation of PIAs. That having been said, the OPC is quoted in *Government On-Line 2005: From Vision to Reality ... and Beyond* as saying:

> "no other government initiative since the enactment of the *Privacy Act* itself has made as significant a contribution to fostering a privacy-sensitive culture within the federal public service"[36]

Room for Improvement

There were a range of possible future developments outlined by the oversight agency, central agency and practitioners. These could be summarised as follows:

Consideration of strategic level PIAs.

There was a feeling that PIA processes in departments and agencies could become too 'compartmentalized'. In the context of the conception, design or adaptation of a departmental or an agency project, it was noted that in many cases the impetus for change begins with planned legislation, i.e. that the decision to create or adapt comes from a higher level than the department or agency tasked to carry it out. Equally, such changes often have a ulti-departmental effects/implications. Thus there was an increasing need to consider the cumulative effects of Cabinet/government decisions over a series of departments/agencies, for example, decisions that will result in increased data sharing across departments. In those circumstances, thought needed to be given to the means, mechanisms and instruments required to ensure that those making decisions at a higher level than the programme implementation process are also thinking about privacy.

Additionally, the cumulative effect of programmes initiated by different departments upon citizens also needed to be considered, for example, Department A might undertake a PIA on the privacy impact of programmeme W, but would not take into account the cumulative effect of that collection and use, with the collection and use of personal information in programmes X, Y, Z in other departments. An analogy was drawn between PIAs and Environmental Impact Assessments (EIAs), where the notion of strategic EIAs that take into account both the effect of actors with overlapping policies and responsibilities, and the cumulative effect of separate environmental impacts is more fully developed.

Greater connection between policy and legislation.

It was felt that central agency policy could and should be tied more directly to legislation – for example, the current requirement that the TBS should review departmental and agency personal information banks and ensure that personal information is kept in accordance with s.4-8 of the *Privacy Act* could be reinforced by requiring that departmental and agency submission of personal information banks for approval would require a PIA to be undertaken and submitted at the same time.

Refocusing of PIAs on risk assessment.

It was suggested that the present PIA process did not readily identify risks for the ordinary practitioner. Faced with a series of Yes/No questions, a non-privacy expert is

[36] *Report: Government Online 2005,* p.23. GOL at http://www.gol-ged.gc.ca/rpt2005/rpt_e.pdf

neither in a position to identify the issues, not to effectively resolve them. Equally, where practitioners hire consultants to undertake a PIA, they may not be aware of the extent to which the Report they receive is either comprehensive or appropriate. Thus the PIAs process may begin to evolve into a more risk-focused tool, requiring departments to assess the degree to which their proposed activities are privacy invasive and only then defining the requirements for a PIA, an approach that will require suitable policy and guidelines to identify what the risks are and provide practitioners with mitigation strategies for particular kinds of risks.

Thus, a scaled approach might help address some of the problems caused by the current common use of checklists to decide whether PIA is required, where a lay person and a privacy expert, both looking at the same set of questions, might come to very different conclusions as to whether a PIA was required. It was noted that while the PIA fail safe theory is "If in doubt do one", in practice that became "If I'm not sure, I don't do one". There clearly remain occasions when PIAs should be carried out but are not, although quantifying the extent of default is difficult. A risk assessment approach would tend to bring some of the borderline, or less obviously privacy-invasive governmental activities e.g. project pilots, research projects, public consultations etc., more clearly within the scope of PIAs.

Increasing infrastructure, resources and personnel.

It was suggested that some departments were not as far along in development of infrastructure to support PIAs as others. Certain departments, such as Health Canada, CIC, HRSDC already had a sensitivity to client personal data ingrained in culture, and were thus more receptive to the PIA process. Other agencies, i.e. in law enforcement, and defence, were more security conscious and thus less concerned about privacy issues. It was clear that in the absence of a sound infrastructure for PIAs, backed by an effective management control framework, that policies and guidelines were unlikely to gain much traction. Thus, in practical terms, facilitating the introduction of such an infrastructure was of equal importance to policy development and tool creation. Regulators could play an important role in the PIA process by defining what an ideal infrastructure would look like, and by helping departments and agencies put that in place, perhaps by guidance on the structuring of the necessary processes, advice on team structure and committee composition, and the linking of PIAs to IT/security assessments. Embedding PIAs into the general project, programme or service workflow, as part of a coherent Threat/Risk Assessment would likely significantly increase their effectiveness and quality.

It was noted that there were drawbacks to relying upon consultants or outsiders to undertake PIA work, as they inevitably lacked as effective an understanding of a department's business processing and dataflow as the internal staff responsible for that activity. The importance of creating an in-house capability for undertaking PIAs, and reducing reliance upon external consultants should not be underestimated, and thus ensuring sufficient resources for training was vital.

Encouraging wider consultation.

The degree of consultation taking place depended largely on the level of intrusiveness of the proposed project. Most consultation took place with the OPC, although this was hindered by the backlog in the PIA review process. It was considered that there should be more consultation between departments, as some departments were well ahead of others in developing information infrastructures, and management processes to support the PIA process. As such, it would make sense for others to borrow those tools, templates and frameworks to benefit their own processes, however this was not happening perhaps because of reluctance to share or because departments saw their programmes as being very different. Breaking down that reluctance could facilitate the spread of PIA good practice and innovation.

Encouraging greater transparency and accountability.

It was noted that departments working on a PIA would usually have a Communication plan to advise the public, or the parties targeted by the application, programme or service, of the outcomes, but prior consultation was currently limited. Very few departments were actually posting summaries of their PIAs on line, and those who used them did so more as a general communication tool – a PIA has been conducted, and there were no problems, or if there are problems, they are being addressed. PIA summaries thus tended to be very general, and did not highlight what the risks were or how they would be mitigated. The aim of producing PIA summaries was so that an individual using a government programmeme should be able to clearly understand the privacy implications associated with that programme's use, and be able to make a determination as to whether or not they want to use it. Meeting that goal would at a minimum require departments to produce more detailed summaries. There was also the possibility of developing a central PIA registry at the federal level to permit both greater public scrutiny and oversight by the regulatory agencies.

Reconsidering reporting, review and audit.

It was commonly agreed that PIAs were not always conducted when they should be, or sometimes not conducted at all. Some indication of the possible shortfall in PIAs could be seen in departments who had been submitting 1-3 PIAs per year, but had then introduced a strong management framework for conducting PIAs, and were now looking at submitting 50-75 PIAs a year. While each department has to produce a public Annual Report on its compliance with the *Access to Information* and *Privacy Acts*, which included how many PIAs were conducted, currently only very basic metrics were required - how many PIAs were done and how many were submitted to the OPC. TBS were considering bolstering the reporting requirements, because in their current form they do not serve as an adequate control to ensure that PIAs are done when they should be. Additionally, under new policy proposals (not yet approved), TBS were considering requiring receipt of copies of all PIAs conducted not to review them all, but to facilitate a more effective oversight role.

In terms of PIA review, it was felt that the federal jurisdiction was moving away from mandatory review of PIAs, but would continue to require notification and/or submission of PIA Reports. It was felt that the OPC would be more effective if not required to review all PIAs, but rather to be provided with summary notification by departments that PIAs had been conducted. This would allow the OPC to request and review selected PIAs of particular interest, and to engage in more targeted departmental, sectoral, or government wide compliance audits.

Private Sector involvement in PIAs

None of the parties interviewed were aware of particular interest or real contact from the private sector as regards the public sector use of PIAs. It was noted that the banking and telecoms sectors were involved in work of a similar nature (Royal Bank of Canada and TELUS were mentioned), but there was little evidence of interaction between public and private sectors.

Research

In completing this report, the following individuals were interviewed or contacted for specific information:

Information, Privacy and Security Policy Division, Chief Information Officer Branch, Treasury Board of Canada, Secretariat (the central agency):

- Andrée Morissette, Senior Privacy Policy Officer
- Navrose Austin, Senior Analyst

The Information, Privacy and Security Policy Division provides strategic advice and assistance to government institutions and TBS policy centres on policies, guidelines and standards concerning access to information, privacy, common look and feel (CLF), proactive disclosure, the management of government information, and information technology (IT) security. The Division is responsible for monitoring and renewing the Government of Canada's Information, Privacy and IT Security policies and standards.

Office of the Privacy Commissioner of Canada (the oversight authority):

- Trevor R. Shaw, A/Director General, Audit and Review
- Lindsay Scotton, Audit and Review

The Audit and Review Branch audits organisations to assess their compliance with the requirements set out in the two federal privacy laws. The Branch also analyses and provides recommendations on privacy impact assessment reports (PIAs) submitted to the OPC pursuant to the Treasury Board Secretariat Policy on PIAs.

ATIP Corporate Secretariat, Human Resources and Social Development Canada (a privacy office)

- Tracey Lee Grant, Senior Policy Advisor
- Denis Lapalme, Senior Policy Advisor

In addition, documents provided by these individuals and found on websites were reviewed. These included:

- PIA templates and instructions
- Web pages describing the PIA process
- Annual Reports
- Internet searches of media coverage of incidents cited by interviewees.

<u>Additional materials</u>

Bird, J. (2003). Privacy Impact Assessments: A Guide to the Best Approach for Your Organization, PRIVA-C™
http://www.priva-c.com/includes/pdf/PRIVA-C%20Whitepaper%20-%20Privacy%20Impact%20Assessments.pdf

Government of Canada Legislation Relating to PIAs

Financial Administration Act

Treasury Board Responsibilities and Powers

Responsibilities of Treasury Board

7. (1) The Treasury Board may act for the Queen's Privy Council for Canada on all matters relating to

> (a) general administrative policy in the federal public administration;
>
> (b) the organization of the federal public administration or any portion thereof, and the determination and control of establishments therein;
>
> (c) financial management, including estimates, expenditures, financial commitments, accounts, fees or charges for the provision of services or the use of facilities, rentals, licences, leases, revenues from the disposition of property, and procedures by which departments manage, record and account for revenues received or receivable from any source whatever;
>
> (d) the review of annual and longer term expenditure plans and programs of departments, and the determination of priorities with respect thereto;
>
> […]
>
> (f) such other matters as may be referred to it by the Governor in Council.

Authority under other Acts

(2) The Treasury Board may exercise the powers, other than powers of appointment, of the Governor in Council under

> […]
>
> (f) such of the provisions of any other Act respecting any matter in relation to which the Treasury Board may act for the Queen's Privy Council for Canada pursuant to subsection (1) as may be specified by the Governor in Council.

Delegation

(3) The Governor in Council may, by order, authorize the Treasury Board to exercise all or any of the powers of the Governor in Council under section 41 or subsection 122(1) or (6) and specify the circumstances in which those powers may be exercised.

Privacy Act (R.S., 1985, c. P-21)

Duties and functions of designated Minister

71. (1) Subject to subsection (2), the designated Minister shall

(a) cause to be kept under review the manner in which personal information banks are maintained and managed to ensure compliance with the provisions of this Act and the regulations relating to access by individuals to personal information contained therein;

(b) assign or cause to be assigned a registration number to each personal information bank;

(c) prescribe such forms as may be required for the operation of this Act and the regulations;

(d) cause to be prepared and distributed to government institutions directives and guidelines concerning the operation of this Act and the regulations; and

(e) prescribe the form of, and what information is to be included in, reports made to Parliament under section 72.

Exception for Bank of Canada

(2) Anything that is required to be done by the designated Minister under paragraph (1)(a) or (d) shall be done in respect of the Bank of Canada by the Governor of the Bank of Canada.

Review of existing and proposed personal information banks

(3) Subject to subsection (5), the designated Minister shall cause to be kept under review the utilization of existing personal information banks and proposals for the creation of new banks, and shall make such recommendations as he considers appropriate to the heads of the appropriate government institutions with regard to personal information banks that, in the opinion of the designated Minister, are under-utilized or the existence of which can be terminated.

Establishment and modification of personal information banks

(4) Subject to subsection (5), no new personal information bank shall be established and no existing personal information banks shall be substantially modified without approval of the designated Minister or otherwise than in accordance with any term or condition on which such approval is given.

Application of subsections (3) and (4)

(5) Subsections (3) and (4) apply only in respect of personal information banks under the control of government institutions that are departments as defined in section 2 of the Financial Administration Act.

Delegation to head of government institution

(6) The designated Minister may authorize the head of a government institution to exercise and perform, in such manner and subject to such terms and conditions as the designated Minister directs, any of the powers, functions and duties of the designated Minister under subsection (3) or (4)

II. ONTARIO PROVINCIAL GOVERNMENT

Context

Ontario is one of 10 provinces in Canada and is the most populated with an estimated twelve and a half million residents of Canada's 32 and a half.[37] Just less than two-thirds of Ontario's population is concentrated in extended Golden Horseshoe [which includes the urban centres of Oshawa, Toronto, Hamilton and St. Catharines-Niagara].[38]

While the ON government and its OIPC have been active players in the development of privacy research and legislation in Canada, the principal driver behind the ON PIA policy has been the Ministry of Government Services (MGS), which sees PIAs as a key part of its threat risk management process in the development and supply of government services.

Legislative and Policy Framework

Legislation

Ontario has three pieces of provincial privacy legislation (see Table 1), two general public sector acts, and one act specific to personal health information.

Table 1 – Ontario Provincial Privacy Legislation

General public sector legislation	*Freedom of Information & Protection of Privacy Act* (FIPPA) in force January 1, 1988. Covers all ministries of the Ontario Government and any agency, board, commission, corporation or other body designated as an "institution" in the regulations.	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
	Municipal Freedom of Information & Protection of Privacy Act (MFIPPA) in force January 1, 1991. Covers all municipal corporations, including a metropolitan, district or regional municipality, local boards and commissions.	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm
Personal health legislation	*Personal Health Information Protection Act* (PHIPA) 2004.	http://www.e-laws.gov.on.ca/html/source/regs/english/2007/elaws_src_regs_r07322_e.htm
	Ontario Regulation 329/04 of PHIPA Applies to health information custodians that collect, use and disclose personal health information, whether or not in the course of commercial activities. Recognised as substantially similar to *PIPEDA* in 2005	http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_040329_e.htm

Ontario has yet to pass general private sector legislation recognised as substantially similar to the federal *Personal Information Protection and Electronic Documents Act*

[37] Statistics Canada at: http://www40.statcan.ca/l01/cst01/demo02a.htm?sdi=population

[38] Statistics Canada at: http://geodepot.statcan.ca/Diss/Highlights/Page9/Page9a_e.cfm

PIPEDA, so *PIPEDA* governs most private sector organisations' collection, use or disclosure of personal information in the course of commercial activities in Ontario. However, as PHIPA has been recognised as substantially similar to PIPEDA, health information custodians are exempted from PIPEDA coverage.

Provincial oversight is via the Ontario Information and Privacy Commissioner's Office which is authorised to receive and investigate complaints.

In Ontario, Privacy Impact Assessments (PIAs) are not explicitly provided for in either the FIPPA or the MFIPPA. As such the PIA process used in the Ontario public sector is policy rather than legislation based and discussed under that heading.

PHIPA also does not formally require the use of PIAs by 'health information custodians' but does require, under s. 6(3)(5) of Ontario Regulation 329/04 of PHIPA, that a 'health information network provider' shall perform, and provide to each applicable health information custodian a written copy of the results of an assessment of the services provided to the health information custodians, with respect to

- threats, vulnerabilities and risks to the security and integrity of the personal health information;
- how the services may affect the privacy of the individuals who are the subject of the information.

The PHIPA PIA process is considered separately from the general public sector PIA process, below.

Policy

Since June 1998, a completed PIA has been required prior to approval of *Information and Information Technology* (I&IT) project plans submitted to Ministry of Government Services (MGS) seeking to begin the detailed design phase or requesting funding approval for product acquisition or system development work, where those projects involve changes in the management of personal information held by government programmes, or otherwise affect client privacy. In December 1999, the Ontario *Privacy Impact Assessment Guidelines* were approved and finalised, and following an update in 2001, are now being used to assess privacy implications in I&IT projects dealing with personal information within the government.[39]

> This requirement ensures that the privacy of individuals is an integral component in the design of new service delivery, technology or information systems, not only at the beginning but also throughout the development and maintenance life cycle of these projects across the government. This approach is intended to preclude inappropriate investments in strategies and development work, and the need to substantially revise such projects.

It appears from discussions at the MGS that recent policy changes anticipate expansion of PIA processes to a wider range of circumstances, including those where funding is not being sought. At the time of writing, an updated set of PIA Guidelines are being prepared (see below), but these are not yet publicly available.

According to the 2001 version of the PIA materials, prior to receiving MGS approval of I&IT projects, sponsoring ministries are required to have their initiatives reviewed by and receive approval from the Architecture Review Board (ARB). The ARB is a key decision-making body in the government's I&IT Organization and is responsible for the ongoing management and development of the Enterprise Information and Information

[39] *Privacy Impact Assessment A User's Guide* (2001) Access & Privacy Office, Ministry of Government Services at: http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf

Technology Architecture (EIA) framework, long range planning for I&IT standards and linkages to the Cluster Architectures/Infrastructure across the government of Ontario.

The EIA framework is based on the Zachman Framework, an integrative framework for managing change in large organisations widely used in federal departments and other government jurisdictions in Canada, used in this case to assist project managers and system designers in their development of I&IT projects.

The ARB requires a PIA to be prepared for I&IT projects as part of its approval process to ensure that privacy issues and concerns are fully identified, documented and addressed. See **Diagram 1** below.

It should be noted that recent developments in Ontario in 2005-2007, including the creation of the MGS from elements of the former Management Board Secretariat, the former Ministry of Consumer and Business Services and the Centre for Leadership and Human Resources Management have resulted in major changes to both the structure of the government in this area, and the adoption of new project management processes. Publicly available documentation of those processes is extremely limited, but it appears that for I &IT projects the new model for project review is based on the Gateway Process developed by UK Office of Government Commerce (OGC)[40] which requires:

- short, focused, independent peer reviews at key stages
- development in partnership with team and stakeholders
- reviews by designated, trained reviewers
- highlighting of risk issues that might threaten project
- gateways to coincide with end of each major project phase

It is not clear at present for PIA purposes whether this model will purely focus on process – e.g. has a suitable PIA been done at particular gateways - or whether it will involve a substantive examination of the analysis and conclusions contained in a PIA.

The central agency responsible for Ontario government privacy policy is the Access & Privacy Office, Ministry of Government Services (hereafter referred to as "the central agency") which administers and interprets the policy and which provides advice to institutions. The Ontario PIA process is very much seen as part of/complimentary to the Threat Risk Assessment process, and is designed primarily to aid management decision-making processes:

> …the PIA is not designed to dictate specific courses of action, or to curtail the sponsoring ministry's range of options in terms of program design or technology options. The function of the PIA is simply to ensure that privacy risks associated with a given proposal are properly identified and addressed wherever possible, and that decision-makers have been informed of these risks and the options available for mitigating them.[41]

There is thus, perhaps, a slightly different focus to PIAs in Ontario than may be found in other jurisdictions.

[40] OGC Gateway Review for Programmes & Projects, UK Office of Government Commerce (OGC) at: http://www.ogc.gov.uk/what_is_ogc_gateway_review.asp

[41] *Privacy Impact Assessment Guidelines*, p.19.

Examples of scenarios where the Ontario policy would/would not require a PIA are laid out in the following table:

Table 2 – PIA decision scenarios

Scenario	***Example***	***PIA***	***No PIA***
Minor Changes to Existing Programmes	Collection of additional eligibility data authorised by statute and reflected in revised notices or consents, or approved data matching agreements		**X**
Major Changes to Existing Programmes	Increase in the scope of collection, use and disclosure of personal information, through programme integration, broadening of target populations	**X**	
	Significant shift toward indirect collection of personal information	**X**	
	Expansion of data collection for new eligibility criteria or programme administration functions	**X**	
New Programmes	New programmes involving significant collection, use, or disclosure of personal information	**X**	
Out-sourcing	Personal information collected for the programme not linked to non-programme personal information or used for non-programme purposes Government will retains control of and accountability for the personal information Appropriate security and compliance verification measures in place		**X**
	Outsourcing delegates operational decision-making power regarding delivery channels and customer service systems	**X**	
Integrated Programme Delivery	If this involves the integration of personal information collected for distinct legislative programmes	**X**	
Technology	Routine system maintenance such as minor software upgrades or patches.		**X**
	Replacement of equipment without significant changes to information management functions/system security		**X**
	Major upgrades to systems and operating systems that change the functionality of information management, access protocols, records indexes or security features	**X**	
	Linking separate programme databases, or creating files that index or point to the personal information on such databases	**X**	
	Changes that affect access channels to personal information by programme administrators, customers or third parties e.g. via the Internet, or kiosks	**X**	

Departments and agencies are not required to provide copies of their assessments to the Ontario Information and Privacy Commissioner, nor are they required to publicly publish either their PIA reports, or summaries of those reports.

The Ontario PIA Process

The central agency provides a certain amount of information, including policy documents, guidance, and tool, the majority of which are accessible via its website.

Table 3 – Ontario government central agency PIA policy, guidance and templates

	Purpose	***Available at***
Draft Model Cross-Jurisdictional PIA Guide (10/1999)	Framework for the completion of a Cross-Jurisdictional PIA, including: checklist for when a PIA is required; goals of a PIA; process overview; data flow analysis, privacy analysis, risk management plan. *This does not appear to be a 'live' document.*	http://www.accessandprivacy.gov.on.ca/english/pub/fed_pia.pdf
PIA User's Guide (06/2001)	Sets out policy requirements, roles and accountability, monitoring and oversight. Also contains Framework for the completion of a PIA, including: checklist for when a PIA is required; goals of a PIA; process overview (Resource Requirements, Documenting Data Flows, Privacy Analysis, Privacy Impact Analysis Report).	http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf
PIA Screening Tool (undated)	Brief questionnaire which project, programme or initiative personnel can use to request an evaluation of whether their project, programme or initiative will require a PIA.	http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.pdf

The number of aids available to those carrying out PIAs is relatively limited. The materials available are not as sophisticated as those available at the federal level, and are not as easy to locate.

The Tool

The central agency publishes two standard tools for the conduct of PIAs:

1. Privacy Impact Assessment Screening Tool
2. Privacy Impact Assessment User's Guide.

The User's Guide contains a PIA Toolkit, which comprises:

- A set of charts for undertaking a data flow analysis, which aim to provide generate comprehensive documentation of data flows through business process diagrams, identify specific personal data elements or clusters of data, and identify potential privacy risks that will require solutions.
- A privacy compliance questionnaire which provides a series of questions derived from the statutory requirements of FIPPA/MFIPPA (with some questions linked to particular sections of the Act) and from the ten fair information practices in the CSA Model Privacy Code. The yes/no/not applicable answers are augmented throughout the form with space to explain.

The PIA process overview describes the PIA as follows.

> A privacy impact assessment (PIA) is a process that helps to determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements. It measures both technical compliance with privacy legislation -- such as the Freedom of Information and Protection of Privacy Act (FIPPA) or the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the broader privacy implications of a given proposal.
>
> … The end result of the PIA process is documented assurance that all privacy issues have been appropriately identified and either adequately addressed or, in

the case of outstanding privacy issues, brought forward to senior management for further direction.

It divides the PIA process into the three stages shown in the table below.

Table 4[42] - Ontario 3-stage PIA process

Conceptual Analysis	***Data Flow Analysis***	***Follow-up Analysis***
Prepare a plain language description of the scope and business rationale of proposed initiative Identify in a preliminary way potential privacy issues and risks, and key stakeholders Provide a detailed description of essential aspects of the proposal, including a policy analysis of major issues Document the major flows of personal information Compile an environment issues scan to review how other jurisdictions handled a similar initiative Identify stakeholder issues and concerns Assessment of public reaction	Analyze data flows through business process diagrams, and identify specific personal data elements or clusters of data Assess proposal's compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Analyze risk based on the privacy analysis of the initiative, and identify possible solutions Review design options, and identify outstanding privacy issues/concerns that have not been addressed Prepare response for unresolved privacy issues	Review and analyze physical hardware and system design of proposed initiative to ensure compliance with privacy design requirements Provide a final review of the proposed initiative Conduct a privacy and risk analysis of any *new changes* to the proposed initiative relating to hardware and software design to ensure compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Prepare a communications plan

Although the PIA process is, in principle, intended to ensure that the "*privacy of individuals is an integral component in the design of new service delivery, technology or information systems, not only at the beginning but also throughout the development and maintenance life cycle of these projects"* the actual process laid out in the Toolkit does not currently appear to reflect an 'end-to-end' approach. It is fair to say that if a PIA Report is completed effectively using the Toolkit, and is then readily accessible to departmental users in the future, to be built on by future PIAs as the system/programme/ technology matures, then it will serve that purpose, However, the task of updating and archiving PIA Reports is not covered in the User Guide.

Completion of PIAs

By Whom?

In principle, the completion and maintenance of PIAs is a shared role involving project managers, policy and programme design staff, systems analysts, security analysts and sponsors. In practice, the work may be carried out by an individual within the project; a team drawn from the project including programme design staff, systems analysts and security analysts; or consultants hired to liaise with the project team

[42] *Privacy Impact Assessment Guidelines*, p.24.

and analyze the project from an impartial standpoint. There is not a great deal of formal guidance from the MGS, and no obvious consensus as to what would constitute good practice.

When?

It is clear from the linkage of the PIA with Threat Risk Assessments in the Ontario governmental system that PIA tasks are intended to be carried out iteratively from the conception of the project to the point of implementation.

> While the completion of a full and detailed PIA may only be possible at later stages in the system development and acquisition phase, the PIA is best approached as an evolving document, which will grow increasingly detailed over time.[43]

External Consultation

While external consultation, in the sense of consultation with the general public, is encouraged, it is not mandatory, and the extent to which it takes place in many departments/agencies appears limited. Given that the User Guidelines state that a key part of the conceptual analysis is:

> An assessment of the public reaction towards the proposed initiative regarding its implications for the protection of their personal information. … Assessing the public's reaction toward a proposal can assist decision-makers in anticipating broader public reactions, and help identify what steps need to be taken to improve overall acceptance.
>
> …
>
> Depending on the type of initiative being proposed or the level of complexity involved, ministries may find it useful to consult broadly with the public or narrowly with key stakeholders.[44]

it is worth considering how those carrying out the PIA intend to take into account public reactions, if they do not consult with either the public or public representatives. Most consultation that takes place is internal, although departments/agencies may consult with the OPC, other provincial and federal departments/agencies, private consultants, and private contractors who will be providing or facilitating services.

Review/Approval of PIAs

Internal

While PIA reports must be signed off by the Deputy Minister of the sponsoring ministry, there is little formal guidance on internal review processes - the User Guide states that:

> *… sponsors may find it useful to designate a senior level project team member as the privacy lead or project privacy manager (PPM). The PPM should have a clear mandate to participate in or review the project design decisions against the criteria of the PIA, and provides ongoing advice and feedback to the senior project management team.*

However, there is not a great deal of evidence that such formal review processes are commonplace.

[43] *Privacy Impact Assessment Guidelines*, p.11.

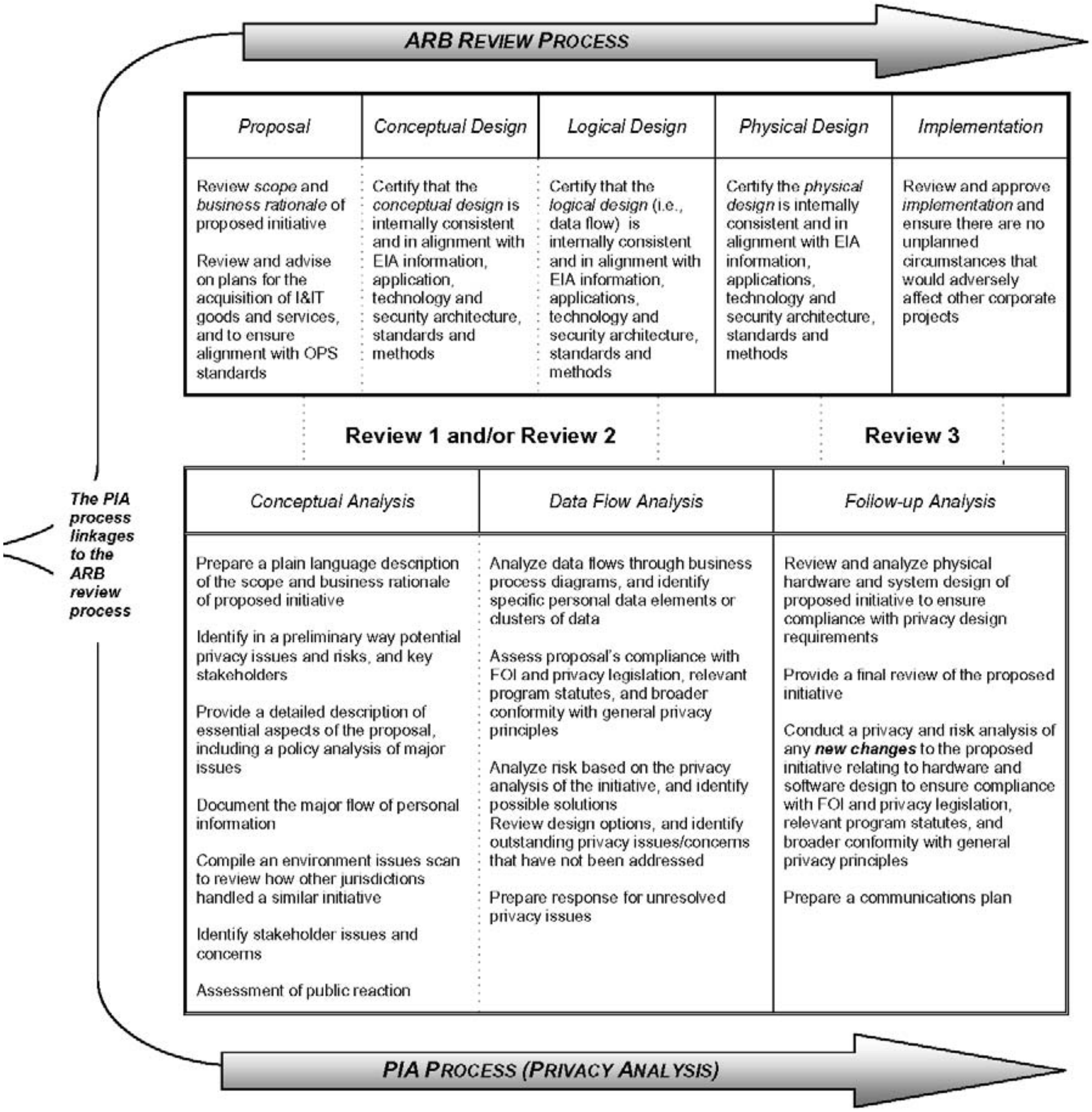
[44] *Privacy Impact Assessment Guidelines*, p.27.

Central Agency Review

As noted above, PIA Reports by departments and agencies are subject to review by the ARB in the MGS, prior to approval by the MGS. The ARB process is intended to run in parallel with the PIA Review process as the project develops towards implementation.

Diagram 1. Architecture Review Board and PIA Review Process[45]

© Queen's Printer for Ontario, 2001



ARB REVIEW PROCESS

Proposal	*Conceptual Design*	*Logical Design*	*Physical Design*	*Implementation*
Review *scope* and *business rationale* of proposed initiative Review and advise on plans for the acquisition of I&IT goods and services, and to ensure alignment with OPS standards	Certify that the *conceptual design* is internally consistent and in alignment with EIA information, application, technology and security architecture, standards and methods	Certify that the *logical design* (i.e., data flow) is internally consistent and in alignment with EIA information, applications, technology and security architecture, standards and methods	Certify the *physical design* is internally consistent and in alignment with EIA information, applications, technology and security architecture, standards and methods	Review and approve *implementation* and ensure there are no unplanned circumstances that would adversely affect other corporate projects

Review 1 and/or Review 2

Review 3

Conceptual Analysis	*Data Flow Analysis*	*Follow-up Analysis*
Prepare a plain language description of the scope and business rationale of proposed initiative Identify in a preliminary way potential privacy issues and risks, and key stakeholders Provide a detailed description of essential aspects of the proposal, including a policy analysis of major issues Document the major flow of personal information Compile an environment issues scan to review how other jurisdictions handled a similar initiative Identify stakeholder issues and concerns Assessment of public reaction	Analyze data flows through business process diagrams, and identify specific personal data elements or clusters of data Assess proposal's compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Analyze risk based on the privacy analysis of the initiative, and identify possible solutions Review design options, and identify outstanding privacy issues/concerns that have not been addressed Prepare response for unresolved privacy issues	Review and analyze physical hardware and system design of proposed initiative to ensure compliance with privacy design requirements Provide a final review of the proposed initiative Conduct a privacy and risk analysis of any ***new changes*** to the proposed initiative relating to hardware and software design to ensure compliance with FOI and privacy legislation, relevant program statutes, and broader conformity with general privacy principles Prepare a communications plan

The PIA process linkages to the ARB review process
PIA PROCESS (PRIVACY ANALYSIS)

[45] Image from *Privacy Impact Assessment Guidelines*, p.84.

Oversight Office Review

The Ontario OIPC has no formal role in the oversight of PIA Reports, but will offer advice and guidance if approached by departments and agencies.

External Review

PIAs are not subject to external review in ON.

Public Availability

Completed PIA Reports are not generally made publicly available; in part because they are largely seen as aids to management, and also because there has been no significant pressure upon the provincial government or MGS from any source to make them available to the public. They would be accessible to the public on request under the Provincial Freedom of Information law (subject to redaction under appropriate exemptions).

Ontario Review and Revision

Background

The Ontario Public Service uses a shared services model where a ministry or agency will undertake the processing of data, or other activities and initiatives, on behalf of a number of other ministries. The aim is to consolidate common corporate administrative systems and functions among departments and agencies to improve efficiency, effectiveness and to lower costs of service delivery. To achieve this effectively, Ontario Shared Services (OSS) was created through the merger of the Shared Services Bureau and the Procurement Policy and Information Technology Procurement Branch of the Office of the Corporate Chief Information Officer in mid-2004.

Between October 2003 and December 2004, Ontario Shared Services (OSS) contacted the OIPC about 11 privacy issues, including the disclosure of privacy issues arising during the processing of Ontario Child Care Supplement (OCCS) cheques. In December 2004, following investigations by the OIPC, a report was issued by the Commissioner making a number of recommendations, including that there should be a privacy review of the operations of the OSS. This was carried out by Deloitte and Touche LLP in the period February - June 2005. Part of that review considered the role of Privacy Impact Assessment - Threat Risk Assessment (PIA-TRA). It identified business processes, systems and the technology applications supporting them. Existing PIA-TRA assessments were then reviewed and evaluated, and additional PIA-TRA assessments were undertaken. The Assessment was conducted from March 28 through June 30, 2005.

The objective of the PIA-TRA review was, amongst other things, to:

- Identify the systems for which recent PIAs-TRAs had been completed
- Review the content of the PIA/TRA for completeness and relevancy
- Assess the validity of the conclusions reached in the PIA-TRA based on the analysis performed
- Identify systems and processes for which PIAs-TRAs had not been undertaken
- Recommend those systems and processes that require the completion of PIAs-TRAs undertaken

In August 2005, a report was released.[46]

Findings of the Review in relation to PIAs

It was confirmed that PIAs and TRAs had been performed for a number of OSS systems and processes. The PIAs reviewed by Deloitte were completed internally by OSS staff and, with one exception, contained fairly detailed descriptions of the personal information involved. Deloitte noted, however, the privacy analysis sections of the PIAs were usually completed at a very high level and, with one exception, were not in conformance with the MBS guidelines. In some cases, the documents required to complete the PIAs did not accompany the Report. Certain PIAs appeared out-dated, given that the services being offered by OSS had undergone extensive modifications by the time of the Deloitte review, and the date of the PIAs. Based on the documentation reviewed, Deloitte suggested that the systems or applications covered by those PIAs were likely to include additional functionality or linkages to other systems/applications that had not been assessed. There were clear deficiencies identified in the preparation of PIAs on a timely basis and in not identifying privacy issues at an early stage in business process programme initiatives. It was also judged that the scope of many PIAs was too narrow as they tended to address just the effects within the IT component rather than the entire business process affected by a proposed change.[47] In conclusion, Deloitte pointed out that PIAs were being performed using the CSA Model Code, on which the federal PIPEDA private sector legislation is based. This was despite the fact that OSS had its own defined Privacy Standard. It was suggested that using the CSA Model Code as a benchmark in the PIA process, thereby effectively using two different privacy standards within the OSS, was unhelpful.[48]

It was recommended that:

- It be mandatory that a PIA/TRA be prepared and reviewed before any change is made to a business process that collects, uses, discloses, disposes or retains personal information within OSS.
- PIAs/TRAs within the OSS should be based on business processes, government programmes and corporate initiatives to ensure that all uses of personal information, not just those with information technology or systems implications are reviewed.
- When the OIPC issues new guidance or directions that affect OSS operations, all PIAs and TRAs should be reviewed to ensure that the new guidance is reflected.
- As the OSS Privacy Standard was developed for use by OSS for dealing with privacy issues, it should be used as the benchmark for PIA/TRA assessment, and the 2001 Guidelines should be updated to reflect the use of the OSS Privacy Standard as a matter of urgency.[49]

Direction of Change

At present there is no obvious sign from the MGS materials that the recommendations of the Deloitte OSS Report have been implemented. The User's Guide is under review, and a new edition is promised, but at the time of writing, it has not yet appeared.

[46] *Ontario Shared Services Privacy Review*, Deloitte & Touche LLP, Ministry of Government Services at: http://www.gov.on.ca/MGS/graphics/052931.pdf

[47] *Ibid* at p.28.

[48] *Ibid* at p.33.

[49] *Ibid* at p.34.

Other PIA Tools and Processes in Ontario

PIAs under PHIPA

As noted in the Legislative and Policy Framework section above, some PIAs are being carried out in relation to the *Personal Health Information Protection Act* (PHIPA) 2004. For the majority of those covered by PHIPA - 'health information custodians', defined in s.3 (1) PHIPA as " …a person or organization described in [s.3] who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work…" PIAs are not mandatory, but are recommended, and promoted heavily, by the OIPC.

For a small group of organisations covered by PHIPA - 'health information network providers' defined in s.6(2) of Ontario Regulation 329/04 of PHIPA as "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians" s.6(3)(5) of Ontario Regulation 329/04 of PHIPA requires them to perform, and provide to each applicable health information custodian a written copy of the results of an assessment of the services provided to the health information custodians, with respect to:

- threats, vulnerabilities and risks to the security and integrity of the personal health information,
- how the services may affect the privacy of the individuals who are the subject of the information.

While this is not formally described as a PIA, it is clearly intended to perform the same, or a similar, function.

The OIPC published a set of PIA Guidelines for the *Personal Health Information Protection Act in October 2005.*[50] These describe PIAs as:

> a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy. A PIA also identifies ways in which privacy risks can be mitigated.[51]

The guidelines suggest that PIAs can help identify particular areas of privacy risk in the health care sector including:

- New technology or the convergence of existing technologies, e.g. an electronic medical record (EMR) system or electronic health record (EHR) system;
- Use of a known privacy-intrusive technology in new circumstances, e.g. the installation of CCTV in patient examination rooms for teaching or educational purposes or the recording of telephone consultations with patients;
- New programmes or changing information handling practices with significant privacy effects, e.g. a proposal to use personal health information collected for treatment purposes to develop a research database or a proposal to integrate an EMR or EHR with a patient scheduling system;
- Legacy systems that may not support privacy and security best practices.[52]

[50] PIA Guidelines for the *Personal Health Information Protection Act in October 2005*, Office of the Information and Privacy Commissioner at: http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf

[51] *Ibid* at p.4.

[52] *Ibid*.

The benefits of PIAs are described as:

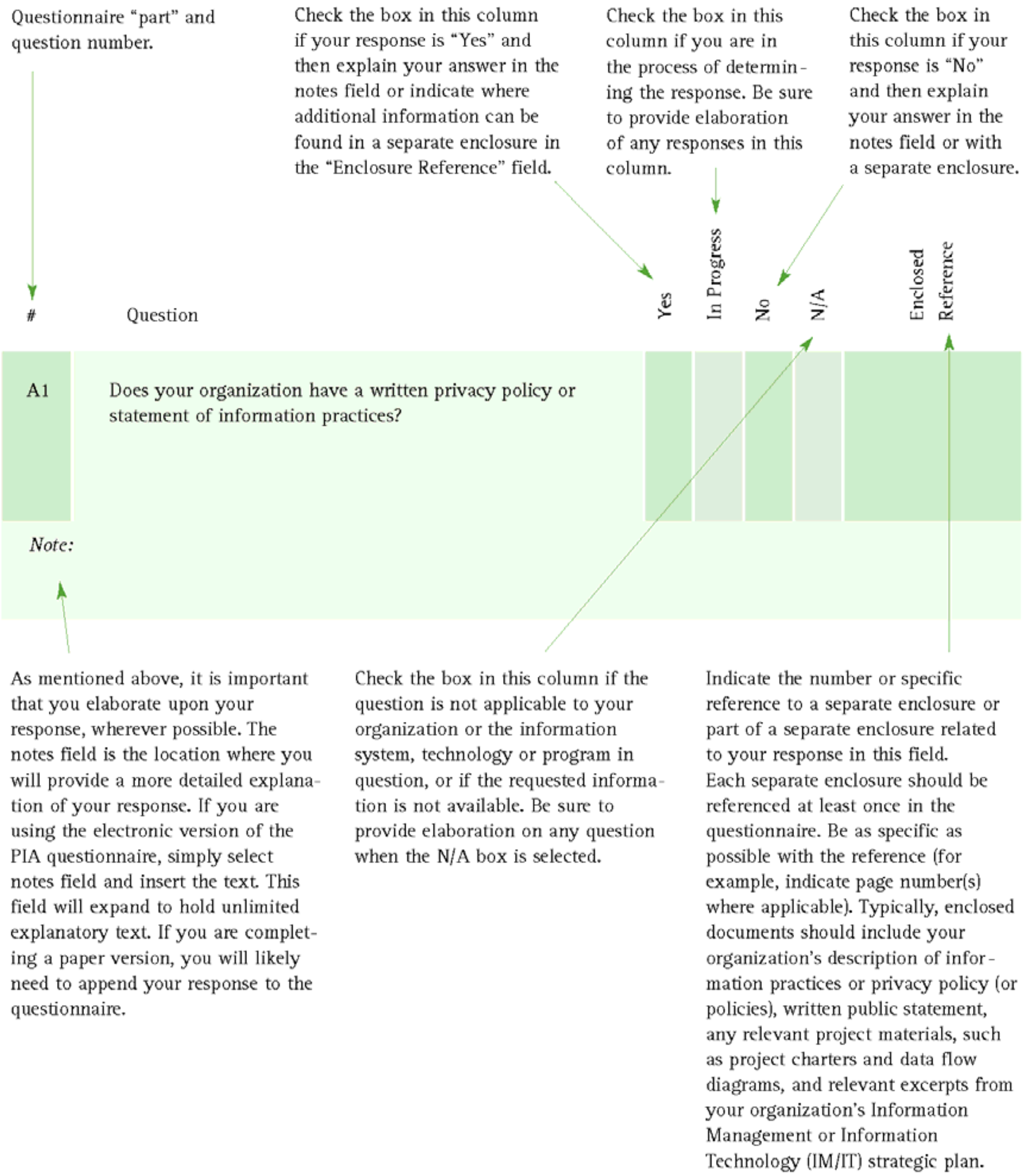
- Outlining data protection risks, which health information custodians are required to mitigate under *PHIPA*.
- Promoting the systematic analysis of privacy issues in order to inform debate on proposed or existing information systems, technologies or programmes;
- Helping relevant decision-makers understand the risks associated with a proposed or existing information system, technology or programme, thus avoiding any adverse public reaction;
- Acting as an "early warning device" to protect the reputation of the health information custodian considering implementing a new information system, technology or programme;
- Bringing responsibility clearly back to the proponents of the proposed or existing information system, technology or programme, to "own" and mitigate any adverse privacy effects;
- Reducing costs when completed at the development stage as changes to meet privacy concerns are cheaper at the design and early implementation phases;
- Providing a credible source of information for health information custodians, privacy regulators, and the public – a PIA can allay privacy concerns that might develop if no credible or detailed analysis were to be available;
- Providing a cost-effective means for privacy regulators to understand the data protection implications of a proposed or existing information system, technology or programme without having to undertake expensive field research themselves.[53]

The Guidelines provide an annotated questionnaire for health information custodians subject to *PHIPA*. It requests information of two general types: that related to the health information custodian's organisational privacy management practices (10 questions) and that related specifically to the information system, technology or programme (20 questions). The questions are similar in format and general content to the PIA questionnaire produced by the Alberta Information and Privacy Commissioner. While there are differences between provincial health information laws, the ON OIPC recognises that organisations in the health sector will want to use PIA tools that are consistent across jurisdictions, as personal health information is likely to be transferred across provincial borders.

The layout of the questionnaire is worth considering in more detail because of the level of detail required.

[53] *Ibid* at 5.

Diagram 2 – Components of the Questionnaire[54]



Does your organization have a written privacy policy or statement of information practices?

Questionnaire "part" and question number.

Check the box in this column if your response is "Yes" and then explain your answer in the notes field or indicate where additional information can be found in a separate enclosure in the "Enclosure Reference" field.

Check the box in this column if you are in the process of determining the response. Be sure to provide elaboration of any responses in this column.

Check the box in this column if your response is "No" and then explain your answer in the notes field or with a separate enclosure.

As mentioned above, it is important that you elaborate upon your response, wherever possible. The notes field is the location where you will provide a more detailed explanation of your response. If you are using the electronic version of the PIA questionnaire, simply select notes field and insert the text. This field will expand to hold unlimited explanatory text. If you are completing a paper version, you will likely need to append your response to the questionnaire.

Check the box in this column if the question is not applicable to your organization or the information system, technology or program in question, or if the requested information is not available. Be sure to provide elaboration on any question when the N/A box is selected.

Indicate the number or specific reference to a separate enclosure or part of a separate enclosure related to your response in this field. Each separate enclosure should be referenced at least once in the questionnaire. Be as specific as possible with the reference (for example, indicate page number(s) where applicable). Typically, enclosed documents should include your organization's description of information practices or privacy policy (or policies), written public statement, any relevant project materials, such as project charters and data flow diagrams, and relevant excerpts from your organization's Information Management or Information Technology (IM/IT) strategic plan.

The guidelines are available as a paper document and in electronic format, and the questionnaire is also available on CD-ROM.

The Guidelines and questionnaire reflect two increasing trends amongst regulators:

- Seeking to mature the PIA process by moving away from simple YES/NO checklists towards "telling the story' of the system technology or programme being reviewed, i.e. "why it is being or has been implemented and how it collects, uses, discloses and retains personal health information".

[54] *Ibid* at 11.

- Aiming to accurately represent the legal standards for personal information protection, but also considering the conducting of a PIA where public concerns or privacy expectations warrant it, even if the organisation is confident it is in compliance with relevant privacy legislation.

Lessons Learned

The primary driver for PIAs in ON was the need to support government decision making processes, i.e. for there to be sufficiently detailed project documentation relating to privacy issues to answer questions from senior bureaucrats and ministers at senior management decision-making stages of the project process. This still largely remains the focus in ON government, but current policy is to seek to broaden the use of PIAs outside of purely decision-making processes.

A key lesson drawn from ON was that the way in which PIA processes are implemented depends heavily upon questions such as:

- What do you want a PIA to do?
- What decision-making process is the PIA part of?
- Is that decision making process effective?
- What are the issues you anticipate your PIAs addressing?

In ON the heart of the PIA process is technical compliance with relevant statutes, and the need to be able to describe data flow in ways relevant to privacy analysis, which means documenting over a period of time how information moves through the system, and plotting the relevant points of collection use and disclosure. The analysis flows from statutory requirements, examining the data flow and comparing that data flow at various points with what the statute requires.

There is then the question of the technology choices that are to be made and how those technologies are deployed and configured – this raises privacy issues that are not answered by a neat checklist or a statutory provision. Instead it is the risk inherent in the technology or system that are at issue. This requires consideration of the concerns about data processing that led to the privacy law in the first place,.e.g., even if the project is in technical compliance with the statute are there significant privacy concerns in the choice of technology to be used e.g. biometrics.

The PIA process therefore requires an assessment of risk that covers both the technical legal aspects required by statute and also risk relating to user acceptance/rejection on the part of the public. This means there is a policy component that's not black and white and this requires those undertaking and assessing PIAs to have a relatively sophisticated understanding of those issues. The nature of what you want a PIA to achieve, and the questions you think you want to expose, will also drive who you want to undertake PIAs within an organisation, and determine the nature of the training that they will require.

It was noted that the role of the PIA tool could easily be overemphasised. The way in which the tool in ON was written was based on the fact that its creators were aware that most potential users would be coming to it cold, thus the PIA tool was as much an educational tool, as it was a process methodology. Designing a successful PIA process was not about the tool used, it was about the privacy management process – the tool was an aid to structuring the documentation of the decisions made during the process. The key element was understanding the whole context within which a tool is going to be used, and the people who are going to use it – the amount of support required for a PIA process will be large if you want to use that process in a sophisticated way and really help decision makers.

In an effective PIA, the need to capture the relevant facts is vital, as is the quality of analysis. Undertaking the kind of analysis required may not be familiar to technical people e.g. observing simple data flows in a system over time and mapping that in a simple process diagram. The way that a PIA tracks information flow needs to be integrated into IT project processes, thus drawing PIA observations and analysis and conclusions into the decision making process. This requires thought about how to situate your tool within a decision making process, and how it relates to your privacy management generally.

The nature of the PIA process, with early consideration of the privacy implications of new developments, often means that it can be difficult to identify in a completed PIA Report the extent to which the project, programmeme or service has been influenced by the assessment. A PIA Report itself might not change the design of project, more usually it is the discussion around the table during the documentation of the project that causes changes. An example in ON was the ON government strategy with regard to the roll-out of PKI –based government services, discussion during the PIA process played a large role in determining how PKI-based services were deployed, including the decision not to implement PKI in citizen-facing services, but only for specific internal governmental processes.

Room for Improvement

The Ontario PIA process is currently in flux, not least because of the recent major government re-organisation, and the role of PIAs is being re-assessed. However, there are some clear issues that arose out of the materials and interviews. These could be summarised as follows:

The role of the OIPC

It was felt that more involvement in the oversight process would be advantageous, although that did not extend to a wish to see mandatory review, as currently occurs at the Canadian federal level. The current hands-off approach was adopted when PIAs were introduced because of the nature of the use of PIAs as a senior management decision-making support tool – it was expected that projects would consult with the OIPC where privacy concerns were raised to avoid difficult questions at the decision point. There was some surprise that the OIPC were not more curious, although the OIPC has input both to projects on an advisory basis and through the ON Independent Advisory Committee which advises on the implementation of the e-Ontario Strategy. It was felt that a useful role for the OIPC would be in terms of oversight of the relative mix of technology and policy protections in government systems e.g. whether privacy was best served by hardwiring data privacy into the design of systems, thus foreclosing some future options (not allowing function creep), or by allowing currently unutilised technological capacity to be built in and constraining it by policies. On that basis the type of PIA oversight being suggested at the federal level, where the OPC was notified of and able to access PIAs, to conduct review of departmental, sectoral or government-wide developments, was a potential way forward, as it would increase awareness of the OIPC of I& IT/electronic government strategies.

Consultation, Consultants and Transparency.

The value of consultation depended in part upon the nature of the PIA process. If PIAs were focused upon internal due diligence to support decision making processes, the role of public consultation might be less important. However, if the PIA process were more public and transparent, this might well impose a discipline on decision-making processes that would provide better decisions more rapidly. It was suggested that there was a real need to engage with external expertise/utilise external intellectual capacity. This need not be through public consultation (indeed doubts were cast upon how effect public consultation would be, both in terms of time constraints and public interest), but by opening up government IT thinking to external parties, not just vendors, but knowledgeable members of the public who want to participate. Publication of PIAs was suggested to be a desirable goal, although doubts were again cast on the interest of the public in seeing PIAs ('the Ministers' phones are not ringing off the hook') and as PIAs would normally be available under Access to Information laws, it was suggested that simply publishing summaries would serve little useful purpose.

Organisational issues

It was noted that ministries do report having problems with conducting PIAs – common complaints include that they are onerous, or difficult to do. A key problem to address is increasing the intellectual capacity of organisations to undertake PIAs, and there are cultural issues around whether organisations want to invest time and resources in making necessary changes and developing appropriate training. The absence of a perception that privacy is of real importance to the public is a real part of the problem in terms of obtaining traction internally.

It is important to deal with privacy issues within organisations in terms of identifying competencies, identifying or creating appropriate organisational positions, and actually formalising privacy work into positions. In the ON government, for example, privacy work is currently largely undertaken by Access to Information and Privacy co-ordinators, which is undesirable as they are focused heavily/primarily upon Access to Information demands. Thus within the ON government there is a need to consider the development of new positions, perhaps linked to security architects/offices. This will need to take place as part of a redefining of organisational roles so privacy management can be effectively situated in the wider context of information management.

While using consultants can bring a helpful degree of objectivity, particularly to internally politicised projects, PIAs are usually more effective if they live with and evolve alongside their projects, and using consultants may hinder the goal of increasing an organisation's internal capacity for carrying out PIAs. Other mechanisms for obtaining objective analysis of whether the project PIA choices made have been documented, and are rational and defensible, include in-house provision of expertise In the ON government a new internal PIA Centre of Excellence has just been established to provide help and consultancy on PIAs on an internal charge-back basis.

Private Sector involvement in PIAs

The OIPC was aware of PIAs being conducted in the private sector - one particular example mentioned was that of GE where, it was noted, management had utilised its Six Sigma business management tool as the basis for incorporating privacy impact assessment into its business process. MGS did not appear to have been approached by private sector organisations as regards the public sector use of PIAs. Some surprise was expressed that private sector vendors did not appear to be conducting privacy analysis of their products and how they recommend those products be deployed by public sector purchasers. It was suggested that it might be useful for private sector vendors to the public sector to think more about the particularities of privacy in the public sector. It was noted that vendors were still seeking to sell technology solutions to ministries, e.g.

enterprise wide information management applications, Customer Relationship Management databases, identity services etc., without apparently understanding that the structure of government in Ontario made cross-governmental deployment of such technologies difficult. It was suggested that private vendors seeking to sell/deploy their technologies into a public sector environment should be undertaking analysis, including PIAs, of how they think their client might deploy that offering. Providing a PIA for a technology as it might be applied by a ministry would be a competitive advantage when selling into public sector environment, but does not appear to happen as part of the design and marketing of products to the public sector.

Research

In completing this report, the following individuals were interviewed or contacted for specific information:

Office of the Chief Information and Privacy Officer, Ministry of Government Services (the central agency):

- Guy Herriges, Manager, Strategy and Policy

Office of the Information and Privacy Commissioner (the oversight authority):

- Ken Anderson, Assistant Privacy Commissioner

In addition, documents provided by these individuals and found on websites were reviewed. These included:

- PIA templates and instructions
- Web pages describing the PIA process
- Annual Reports
- Internet searches of media coverage of incidents cited by interviewees.

Policy Extract

Ontario Regulation 329/04

Section 6(3)

…

5. The provider shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to,

> i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and
>
> ii. how the services may affect the privacy of the individuals who are the subject of the information.

III. ALBERTA PROVINCIAL GOVERNMENT

Context

Alberta is one of 10 provinces in Canada's federal system of government, and is the 4th most populated at three and a quarter million residents of Canada's 32 and a quarter. Its two major population centres, Edmonton, the capital, and Calgary, the commercial centre are each over a million in population. The economy is driven by petroleum extraction and agriculture.

Alberta is adjacent to British Columbia in Western Canada and has fairly similar privacy legislation, with the exception of Alberta's specific *Health Information Act*. The two provinces work very cooperatively, particularly with regard to their private sector privacy legislation which became effective at the same time in January 2004.

Legislative and Policy Framework

Legislation

Freedom of Information and Protection of Privacy Act, (FOIP Act)

The applicable public sector privacy legislation governing Privacy Impact Assessments (PIAs) in Alberta is the *Freedom of Information and Protection of Privacy Act,* (FOIP Act), Revised Statutes of Alberta 2000, Chapter F-25.[55] This legislation became effective in October 1995.

The Act applies to public bodies, which include: a department, branch or office of the Government of Alberta; an agency, board, commission, corporation, office or other body designated as a public body in the regulations; Executive Council offices; some offices of Officers of the Legislative Assembly, and local public bodies (educational, health care, and local government bodies).

The FOIPA Act does not mention PIAs, but, according to the Commissioner's website,

> "The FOIP Act provides the authority for the Information and Privacy Commissioner to comment on the implications for freedom of information or for protection of privacy of proposed legislative schemes or programs of public bodies.[under s. 53(1)(f)]. Privacy impact assessments are not mandatory under the FOIP Act, but are recommended for major projects that involve the collection, use or disclosure of personal information." [56]

Arguably, authority exists under the FOIP Act for Cabinet to make regulations relating to the conduct of PIAs, but this has not been utilised.[57]

Alberta also has specific health information privacy legislation, the *Health Information Act*, under which PIAs are mandatory. See more on this below.

[55] Find the FOIP Act in unofficial form on the central agency's website at: http://foip.gov.ab.ca/legislation/act/index.cfm

[56] *PIAs – Description*, from the Office of the Information and Privacy Commissioner of Alberta's website at http://www.oipc.ab.ca/pia/index.cfm

[57] Those sections include sections 94(1):
(k) respecting standards to be observed and procedures to be followed by a public body implementing a program for data matching, data sharing or data linkage; and
(v) respecting any other matter or thing that the Lieutenant Governor in Council considers necessary to carry out the intent of this Act.

Health Information Act (HIA)

The requirement to conduct PIAs is enshrined in section 64 of the *Health Information Act* (HIA), RSA 2000, chapter H-5.[58] The *Health Information Act* (HIA) was passed by the Alberta Legislature in 1999 and came into effect on April 25, 2001. The Act and PIA requirement applies to health information "custodians", or organisations that deliver health care services paid for under the *Alberta Health Care Insurance Act* (which publicly funds many health services).

> "The HIA provides individuals with the right to request access to health records in the custody or under the control of custodians, while providing custodians with a framework within which they must conduct the collection, use and disclosure of health information. Custodians are defined in section 1(1)(f) of the HIA and include:
>
> - The Minister and Department of Alberta Health and Wellness
> - Any health service provider paid in part or in whole by the Alberta Health Care Insurance Plan
> - Pharmacies and pharmacists regardless of how they are paid
> - Regional Health Authorities and provincial health boards (Alberta Cancer Board and Alberta Mental Health Board)
> - Nursing home operators."[59]

Section 64, Duty to prepare privacy impact assessment, sets out the requirement to conduct PIAs:

> **64(1)** Each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.
>
> **(2)** The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

In addition, PIAs are required to be produced and reviewed by the Commissioner under other sections of the Act in specific situations relating to data matching (ss. 70 and 71) and disclosure of personally identifying health information to the health minister or department (46(5)).

This may be the only instance of legislation requiring both production of PIAs and their review by an oversight body.

Personal Information Protection Act (Private Sector Privacy Legislation)

While there is also privacy legislation governing *private* sector organisations (the *Personal Information Protection Act*, S.A. 2003, c. P-6.5) [60], it does not address administrative procedure to the same extent as the FOIP Act and HIA, and does not mention PIAs. In fact, the Alberta Privacy Commissioner cannot recall seeing a private sector PIA, his Office ever requesting one, and only knows of one private sector firm that definitely conducts PIAs in-house. However, he knows of some systems, management,

[58] The Health Information Act is available on-line at: http://www.assembly.ab.ca/HIAReview/Health_Information_Act.pdf

[59] From the Alberta Privacy Commissioner's website at: http://www.oipc.ab.ca/hia/

[60] PIPA is available on-line at: http://www.psp.gov.ab.ca/index.cfm?page=legislation/act/index.html and http://www.qp.gov.ab.ca/documents/Acts/P06P5.cfm?frm_isbn=0779726316

legal and privacy consultants employing proprietary PIA instruments for private sector clients in Alberta, but has not seen a report.[61]

The Commissioner does not foresee his office participating in development of a PIA tool for use by the private sector under PIPA, but it is in favour of PIAs being carried out in the private sector. The Commissioner's Office informally promotes their conduct by private sector organisations. Officers have advised private sector organisations on how and when to conduct PIAs, when approached for advice on development of new programmes or information technology systems (in non-logged telephone conversations). The Commissioner also reports that he has mentioned PIAs in speeches on implementing PIPA and has publicly stated that his reasonableness test, should a matter come before him in inquiry, would consider the conduct of a PIA as an indication of due diligence.

Public Sector Privacy Policy and Guidance Material

Both the central agency and the oversight body provide descriptive material and guidance on completing PIAs, available on their websites. However, in Alberta, the anomalous situation exists where the Oversight Agency is more involved with PIAs than the central agency. Although the central agency includes the policy in its government policy manual, the PIA process and instrument were developed by the Commissioner's office and that office reviews PIA reports.

Alberta regulators publishes two standard tools for the conduct of PIAs:

3. The annotated Questionnaire form is on the Commissioner's website at http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf
4. The central agency publishes PIA policy in its Guidelines and Practices manual. It contains a good description of PIA process in Chapter 9: Privacy Compliance, at http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3

The Commissioner's website[62] states that "Privacy impact assessments are not mandatory under the *FOIP Act*, but are recommended for major projects that involve the collection, use or disclosure of personal information."

Alberta Government policy requires that the development of new systems or the significant enhancement of existing ones that deal with personal information undergo "an extensive review of their impact on personal privacy."[63] This policy is published as Guidelines and Practices. The section on PIAs is part of a chapter on Privacy Compliance.[64] The authority to develop policy in this field derives from the minister's responsibility for the FOIP Act. The guidance material addresses, among other things:

- When to start
- How to pull a team together
- Approval
- Public consultation

[61] An example of consulting companies publicising PIA services on their websites include Cenera at: http://www.cenera.ca/default.asp?tier_1=109&tier_2=148&content=130 ,

[62] Office of the Information and Privacy Commissioner of Alberta, *PIA Description*, at http://www.oipc.ab.ca/pia/index.cfm

[63] Alberta Employment, Immigration and Industry, *Privacy Impact Assessment Primer*, January 2007, p. 2.

[64] 9.3, Privacy Impact Assessments, in chapter 9, Privacy Compliance, Guidelines and Practices, Service Alberta (the central agency for information and privacy), 2005 Edition at http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm

The Alberta PIA Processes

History of the Alberta PIA

The original PIA approach was developed by the Privacy Commissioner, Franklin J. Work and Tom Thackeray, both of whom had environmental management backgrounds. They were aware of an environmental assessment process that existed in the Canada and the USA and thought it could work for privacy. They agreed to use the environmental assessment as the model for the Privacy Impact Assessment for the FOIP Act. This model was also later applied to the *Health Information Act*.

The Commissioner's Office took the lead in developing the template and guidance material, and therefore created the unusual system of oversight agency review, which was accepted by government and adopted as policy. The current version of the PIA template was drafted by Alec Campbell, an access and privacy expert seconded from the central agency to the Privacy Commissioner's office.

The Tools

According to the introduction to PIA Guidance and Processes on the central agency website,

> "A *privacy impact assessment* (PIA) is a process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy. The process is designed to ensure that the public body evaluates the project or initiative for technical compliance with the *FOIP Act* and also assesses the broader privacy implications for individuals. A PIA is both a due diligence exercise and a risk management tool. Although only real breaches of privacy contravene the privacy provisions of the *FOIP Act*, even the perception that privacy may not be adequately protected can seriously damage the reputation of a public body as well as the public's confidence in a particular program or initiative.
>
> The PIA process requires a thorough analysis of the potential impact of the initiative on privacy and a consideration of measures to mitigate or eliminate any negative impact. The PIA is an exercise in which the public body identifies and addresses potential privacy risks that may occur in the course of its operations. While PIAs are focused on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy and security policies and procedures, or the lack of them, can be significant factors in the ability of the public body to ensure that privacy protection measures are available for specific projects.

Downloadable versions of the two forms of the PIA Template and Instructions and an Annotated Questionnaire are available in different software on the oversight body's website[65]. These tools are designed to be used for PIAs under both the FOIP Act and HIA, and are described on the website as follows:

- "The **Full Questionnaire** is for use in all PIAs. This Questionnaire allows a public body or custodian to provide information on both their organizational privacy practices (Part A) and information on the privacy implications of specific programs or projects (Part B).
- The **Supplementary Organization Questionnaire** is for use in projects involving more than one organization. In situations with multiple partners, the primary organization is required to submit a full PIA (using the Full Questionnaire) while the other partners can submit the Supplementary Questionnaire.

[65] Office of the Information and Privacy Commissioner of Alberta, *PIAs, Template*, at: http://www.oipc.ab.ca/pia/template.cfm

- Finally, the OIPC has also created the **Privacy Impact Assessment: Instructions and Annotated Questionnaire** for use while completing PIAs.

The Alberta PIA Questionnaire is essentially an annotated questionnaire or legislative compliance checklist in its format, although the accompanying instructions and description describe a more comprehensive privacy review. It can be completed on paper or electronically. Notes fields provide space for elaboration, and answers can be cross-referenced to attachments.

The Commissioner's website describes the process objectives of its PIA, stating that it should be fairly broad and consider organisation-wide practices:

> "The Office of the Information and Privacy Commissioner has developed a Privacy Impact Assessment (PIA) process to assist organizations in reviewing the impact that the new project may have on the individual privacy. The process is designed to ensure that the public body or custodian evaluates the program or scheme to ensure compliance with the FOIP Act or HIA.
>
> The PIA process requires a thorough analysis of potential impacts on privacy and a consideration of measures to mitigate or eliminate any such impacts. The privacy impact assessment is a due diligence exercise, in which the organization identifies and addresses potential privacy risks that may occur in the course of its operations.
>
> While PIA's are focussed on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy policy and procedures, or the lack of them, can be significant factors in the ability of the organization to ensure that privacy protecting measures are available for specific projects[66]

As described later under Other PIA Tools and Processes in Alberta, one government ministry has developed its own template and process now used by several ministries with the agreement of the Commissioner's Office. The template requires narrative descriptions and answers, rather than taking a checklist format, using a format that British Columbia's current revision is now pursuing.

Completion of PIAs

By Whom?

The PIA tool is designed to be completed largely by the business area (or program staff) originating a project or initiative, in consultation with departmental Privacy Offices and with the participation of a team of specialists.

The PIA process leader would ideally be "someone who understands the *FOIP Act* and privacy principles and issues, has technical writing skills, has project management experience and can synthesise input from a variety of sources."[67]

In the alternative process used by the Department of Employment, Immigration and Industry, the Privacy Office actually completes the PIA report. Its guide, Privacy Impact Assessment Report Development and Sign-Off Process states that:

> "While the Information and Privacy Office will be responsible for writing the assessment report, the responsibility for privacy compliance and the accuracy and completeness of the report content remains with the project sponsor business area."

[66] Introduction, PIAs, Office of the Information and Privacy Commissioner, at http://www.oipc.ab.ca/Search/DetailsPage.cfm?ID=60

[67] From the government (Service Alberta's) PIA Guidelines and Practices, Chapter 9, Privacy Compliance, Privacy Impact Assessments, at: http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3

Who participates?

Guidance is further given to practitioners about establishing a PIA development team, which "could include the FOIP Coordinator, the project or programme sponsor, records manager, project manager, IT/IM specialists, legal services, communications specialist and a senior or executive manager." In addition, "If an information technology system or enhancement involves more than one government department, the Office of the Corporate Chief Information Officer of the Government of Alberta should be consulted in the preparation of the PIA."

Alberta has also seen the trend, observed in British Columbia, of having Information Systems contractors involved in systems development participate in development of the PIA, and this requirement may be stated in solicitation documents. However, while contractors may complete parts and provide information, they are not responsible for the PIAs production – that rests with the ministry or agency.

When and under what circumstances?

Alberta provides a good description of the circumstances under which a PIA should be completed by public bodies under the FOIP Act in 9.3 of its Guidance and Practices on PIAs.

> "Public bodies should consider conducting a PIA when
>
> - new data elements will be collected and added to an existing personal information database, or a new database is proposed;
> - system access will be rolled out beyond current parameters, controls, levels or numbers of users;
> - the use of personal information will be expanded to include data linkage or matching or other purposes;
> - limited disclosure or reporting about selected individuals will be expanded to enable broad disclosure of information about a larger population base;
> - the way in which the system is accessed, managed or secured from a technical or managerial perspective is changed significantly (including use of internet technology or outsourcing); or
> - the retention period for personal information in the system will be changed.
>
> As information systems become more complex, the probability of having an unexpected impact on privacy increases. Initiatives that appear to involve minor technical enhancements for client convenience and public body efficiency may significantly impact individual privacy."

This guidance also states that "a PIA is rarely ever finished. It is a dynamic document that should be updated from time to time as changes are contemplated for the program."

It is the sense of the Alberta central agency that PIAs are not completed in all instances in which they should be completed – that is, public bodies do not complete them for all initiatives for which PIAs are recommended. While the policy is not mandatory, that office feels that education about the policy might result in better voluntary compliance. The office does not see itself recommending legislative changes to impose a non-discretionary requirement to conduct PIAs, but could see itself recommending implementation of such a policy at some time, if needed.

The Commissioner reports that there is no problem convincing public bodies to conduct PIAs, especially when they are undertaking a significant programme. The latest Annual Report (for fiscal year 2005/6) indicates that 16 PIAs were submitted by public bodies under the FOIP Act and seven Privacy Impact Statements (a shortened version of the

PIA used by some ministries). The previous year's report indicated that 13 PIAs were submitted under the FOIP Act.

Under the *Health Information Act*, PIAs must be completed and reviewed by theCommissioner's Office "before a custodian implements proposed administrative practices and information systems relating to the collection, use or disclosure ofindividually identifying health information."[68]

External Consultation

Guidance provided in central Privacy Compliance Guidance and Practices on PIAs speaks to public consultation.

> ***Consider whether public consultation is needed***
>
> "The public body should address in the PIA how it intends to educate and consult with affected stakeholders respecting the proposed initiative. Alternatively, the justification for not consulting should be set out in the PIA."

In practice, consultation appears only to be conducted with regard to the initiative in general, rather than the privacy aspects of it.

The following specific guidance on public consultation is from the alternative Alberta Employment, Immigration and Industry's Privacy Impact Assessment Report Development and sign-off Process guidance document.

> **"Public and Stakeholder Consultation**
>
> Identification of privacy issues must consider the various stakeholders and publics. If known, their views should be provided in the privacy impact assessment report submitted to the Commissioner along with a description of how the views were obtained.
>
> From a strictly legal and technical perspective, Alberta Employment, Immigration and Industry is interested in the following:
>
> - Does the Department have the legislative authority to do what is being proposed?
> - Do the proposed project, and associated business processes, comply *in letter and spirit* with the *FOIP Act*?
>
> If the answer to both of these questions is "yes", there may be some level of comfort in continuing *without* formal public and stakeholder consultation.
>
> It is the Department's intent to include a reference in any public announcement concerning a new project, to the privacy impact assessment that has been done for that project.
>
> The privacy impact assessment report, once reviewed by the Commissioner, is considered a public document. Note, however, that some information of a technical nature may be attached to the assessment report in the form of an appendix that would not be made public. These appendices, if required, should clearly be noted as such."

[68] From the Information and Privacy Commissioner of Alberta website, *PIAs, Description*, at: http://www.oipc.ab.ca/pia/index.cfm

Review/Approval of PIAs

Alberta departs from the norm, in that the oversight office set the process and template, and reviews completed PIAs, rather than the central agency.

Internal Review

Central Privacy Compliance Guidance and Practices states that "The internal approval of a PIA should be based on the public body's established internal approval process and should include approval from the members of the PIA development team." Therefore, the internal sign-off process differs by organisation.

The internal approval process of the department that has its own specific process codified includes: branch, project sponsor; business area (Division); and Deputy Minister approval before the report is sent to the oversight agency for review. The Deputy Minister is the highest civil service official in the ministry, reporting directly to the Minister.

Central Agency Review

There is no requirement for PIAs to be reviewed by the central agency and in practice, ministries do not chose to consult or bring their completed PIAs to the central agency before taking them to the Commissioner's Office. According to the head of the central agency, it does not have much of a role in PIAs. However, departments may come to the central agency for advice on how to address privacy issues for new initiatives, quite apart from the PIA process. Thus, the central agency is a resource of experts but not a formal part of the PIA process.

Oversight Office Review and Acceptance

Review of PIAs

The review of PIAs is a means of obtaining an understanding of the undertaking and its privacy implications of an initiative, to inform the Commissioner's statutory right to comment on programmes under s. 64(2) of the FOIP Act. Since April, 2001, over 1,200 PIAs have been reviewed. Currently, 300-400 PIAs are received a year. About 75% of the PIAs are conducted under the *Health Information Act*, and these are handled by three staff members –, officers serving at the senior manager level.

All PIAs must be reviewed by the Commissioner's Office. The Commissioner has been reviewing and commenting on PIAs since proclamation of the FOIP Act in 1995.[69] PIA reports are sent by the head of the sponsoring organisation to the Commissioner. They are screened by an intake officer who sends them to the director responsible for the particular legislation to which the organisation is subject, and the director assigns them to an officer based on workload or expertise.

In the health area, which receives by far the highest proportion of PIAs, there are staff members with health information technology and health informatics backgrounds, and these people can readily identify issues or practices that do not meet industry standards.

The officer is responsible for determining if the PIA is accepted. The completeness and the quality of the PIA determines the interaction, if any, the officer will have with the organisation.

[69] Office of the Information and Privacy Commissioner of Alberta, *PIAs, Directory* at http://www.oipc.ab.ca/pia/registry.cfm

The following description of what the Commissioner's Office looks for and how the process unfolds, from the practitioner's perspective.[70]

> The Commissioner may comment after reviewing the privacy impact assessment report if it is found that:
>
> - legislative authority for collecting, using and disclosing personal information is unclear or missing; or
> - impacts on privacy are significant and unmitigated; or
> - risks to privacy outweigh the benefits of the project.
>
> If the Commissioner provides comments to the public body, it will be up to the public body to accept the comments and provide clarification or proceed without further review by the Commissioner. The Commissioner may also comment publicly on the project, if he considers such comment to be appropriate.

If the officer is satisfied that appropriate due diligence has been taken, and there is no reason to believe that the initiative is non-compliant, then the PIA will be accepted. A letter is written to the head of the organisation to inform him or her that the PIA has been accepted.

However, if there is insufficient evidence on which the officer can accept a PIA, the officer may write a letter making comments or requesting specific information, or asking the organisation for a presentation or meeting. Most often, interaction is based on written correspondence and formal meetings, but for complex initiatives, it may be a combination of modes of contact including telephone calls. In some instances, the officer might even travel to the premises of the organisation.

In most instances, there are one or more rounds of requests for further information, clarification, or raising issues, before the review is complete and the PIA can be accepted. Changes to the initiative are often made during this exercise. That said, the template is designed to be comprehensive and, if completed properly, there would be no need to follow up.

The Commissioner does not recall significant "push-back" from organisations when his office has identified a privacy issue that should be addressed. Organisations already have a large amount of time, effort and resources invested in the initiative by the time a PIA is submitted.

Some PIAs are sent back after an initial review because they are incomplete – questions in the template have not been answered, or because they have answered questions incorrectly – for instance, assuming the programme has legislative authority to collect personal information when it does not.

For large programmes with significant privacy implications, the OIPC may be consulted regularly, even in draft stages of the PIA's development. In cases where an organisation is well-versed in the conduct of PIAs, the first the Office will learn of an initiative is receipt of the completed PIA.

Acceptance of PIAs

The review, when completed and issues are satisfactorily addressed, results in an "acceptance" of the PIA report, rather than 'approval'. This is an important distinction.

[70] Alberta Employment, Immigration and Industry, *Privacy Impact Assessment Primer*, January 2007, p.2.

In accepting a PIA, the Office is not suggesting that the way in which privacy issues has been addressed by the initiative is optimal, but that reasonable measures have been used and a sufficiently complete process of privacy assessment was conducted.

The following explains what it means for the Commissioner's Office to "accept" a PIA.

> Because the onus always remains on the organization to ensure adequate levels of privacy protection, as required in the applicable legislation, the Commissioner will not "approve" a PIA submitted to him by an organization. Once satisfied that the organization has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner will "accept" the PIA. Acceptance is not approval; it merely reflects the Commissioner's acceptance that the organization has made reasonable efforts to protect privacy. A PIA cannot be used to obtain a waiver of, or relaxation from, any requirement of the relevant legislation. [71]

The fine line between "acceptance" and approval" is maintained by avoiding any prescriptive comments which may later impair the ability to be seen as independently commenting. It is the belief of this oversight agency that is should not provide answers, only express concerns or ask questions.

External Review

There is no system of external review of PIAs apart from the oversight agency, the Information and Privacy Commissioner's Office.

Public Availability

PIAs in Alberta are constructed in two parts: the public and, under separate cover, the one intended to be kept confidential and which might contain in formation on security measures. The Commissioner's office considers PIAs to be public documents and will provide a copy or access to the public part, but would refer a requester to the originating organisation for the confidential part. That said, there is very little demand for PIA reports.

In the annotated questionnaires (the PIA template), the completed PIA is described as a public document.

> The PIA questionnaire will be considered a public document by the Office of the Information and Privacy Commissioner. Enclosures will also be considered public documents, unless they are explicitly designated as "Confidential". Enclosures designated as "Confidential" must be accompanied by the reason(s) for confidentiality. Reasons must be consistent with one or more exceptions to release under Part 1, Division 2 of the FOIP Act.[72]

If someone requests a PIA of a department, an access to records request under Freedom of Information legislation is usually required, and the PIA report will be reviewed by the agency that produced it for the need to sever or redact information whose release would be harmful under specified legislated exemptions to the right of access.

The types of information which may be subject to severing include those that relate to information security, or where disclosure would be harmful to the business interests of a third party. Some ministries follow central policy regarding information system security

[71] Office of the Information and Privacy Commissioner of Alberta, *Introduction – PIAs*, at http://www.oipc.ab.ca/Search/DetailsPage.cfm?ID=60

[72] Office of the Information and Privacy Commissioner of Alberta, Privacy Impact Assessment: *Instructions and Annotated Questionnaire,* page 5, at http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf

and do not outline specifics in the PIA. There have been no cases where severing of a PIA has been the subject of a complaint to the Commissioner's Office.

PIA Registry

The Commissioner's website publishes a list of completed PIAs that have been accepted by the Office, with short summaries. This Registry is available in searchable form on the Commissioner's website.[73]

The "PIA Registry contains a summary of projects that affect the way personal information in collected, used or disclosed within Alberta. The summaries contained in this registry are taken directly from the PIA submitted by the custodian or public body and do not convey OIPC opinion on the programme or project referenced." The summaries describe the initiative for which the PIA was carried out, but do not provide any description of the assessment itself. They are searchable by organisation and keyword, and a "What's New" page lists current year PIAs.

Other PIA Tools and Processes in Alberta

One government privacy office responsible for three large, personal information intensive departments and a central personnel agency had developed its own PIA template that differs from that published by the Commissioner. The head of the privacy office felt that the Commissioner's PIA template "did not flow well". The department's PIA "tells a story" and is more narrative in form.[74] It is the department's policy, and that of the departments it supplies privacy services to, to conduct PIAs for all applicable initiatives, even though they are not strictly required. The privacy Director sees this as "best practice" and part of building a "privacy-conscious culture". The programme areas learn about privacy during the process of conducting the PIA, and the approach is to enable the programmes to carry out their business and not to have privacy get in the way.

The Commissioner is agreeable to the department's PIA tool being used, and his Office is accustomed to reviewing PIAs in this format.

The department produces a series of privacy impact assessment guides including:

- Privacy Impact Assessment Primer (quoted above)
- Content of a Privacy Impact Assessment Report (a template)
- Privacy Impact Assessment Report Development and Sign-Off Process

Accompanying guidance material produced by the department in the form of a "Primer" explains the need for PIAs:

> A Privacy Impact Assessment is a due diligence exercise, in which Alberta Employment, Immigration and Industry identifies and addresses potential risks to individual privacy that may occur in the course of its operations.
>
> Conducting a privacy impact assessment is good business practice. In the same way that financial, legal, operational, and other implications are generally considered prior to proceeding with a project, privacy implications also need to be considered both in the decision to proceed with a project, as well as throughout the project development process itself.

[73] The Alberta Privacy Commissioner's PIA Registry is at: http://www.oipc.ab.ca/pia/registry.cfm
[74] Interview with George Alvarez, Director, Information and Privacy Office, Alberta Employment, Immigration and Industry

The Primer explains the processes to be used in the department, describing when a PIA or a Privacy Impact Statement must be completed. It also provides information that privacy novices need to know, for instance, the difference between privacy and security, and the ten privacy principles, explained within the context of the Alberta and departmental regulatory framework. The process is designed to be used in conjunction with a formal project management process in place in the ministry, and the primary audience is project managers.

The PIA template requires a detailed description of the initiative and its benefits, a description and rationale for personal information collection, use and disclosure, an analysis of the protection of personal information (including a rationale by data element and a personal information flow analysis), and discussion of privacy impacts, including mitigation of impacts.

The document, Privacy Impact Assessment Report Development and Sign-Off Process, walks those conducting a PIA and Privacy Impact Statement (the shorter version for simpler cases), through the entire process, from initial research through writing the PIA report to obtaining approvals.

The privacy office conducts about 35 Privacy Reviews, which include both Privacy Impact Assessments and Statements a year, for the organisations it provides service to, in conjunction with programme areas. It also supports practitioners in the conduct of PIAs with annual half-day workshops on PIAs as part of an annual privacy conference.

In addition to the PIA and PIS templates and guidance material, the department has a number of self-assessment tools: Privacy Framework, PIA, Privacy Scans or Statements (an abridged form of PIA where a full PIA is not warranted, under which the initiative is still analyzed and written it up (about 4 pages) and shared with OIPC).

The Privacy Impact Statement or Scan is conducted "When a review of the project indicates the project has limited scope and there are no significant privacy impacts, there is a decreased need for a formal PIA. A *privacy impact statement* (PIS) is a report of the review that was carried out. A PIS could be used for example, where a new process is created but the use of personal information is minimal." "A *privacy impact assessment* (PIA) is a due diligence exercise, in which Alberta Advanced Education and Technology identifies potential impacts on privacy that may occur from the implementation of a project and considers measures to mitigate or eliminate any such impacts."[75] The PIS is completed by the programme area and reviewed by the department privacy office before being sent to the Office of the Privacy Commissioner. There is no requirement for PISs to be reviewed by the Commissioner's Office.

A template for the PIS and a description of the sign-off process have been produced. The report form is very short, containing space for a:

- Description of the programme objectives and operation
- List of the broad categories of personal information used for the programme
- List of categories of individuals who will be affected by the programme or whose personal information will be collected for the programme
- Summary of uses and disclosures of personal information collected for the programme, including a list of any exchange agreements of that personal information with any outside parties
- Reasons why collection of personal information is deemed essential for the programme

[75] Alberta Advanced Education and Technology, Privacy Impact Scan Sign-off Process, as current, August, 2007.

- Security measures, defined in broad terms, taken to protect the personal information against unauthorised collection, use, disclosure, modification, retention and destruction
- Recommendation of Alberta Advanced Education and Technology regarding whether to proceed with the programme / project, or whether modifications are required

PIA Template and Process Review and Revision

Alberta conducted a revision of its PIA template in about 2003. Currently, there are no plans to revise the template or guidance material. The central agency does not see itself recommending to government that the requirement to conduct PIAs be put in legislation, although it might consider mandating them by policy for certain types of initiatives (in contrast to the current situation where PIAs are merely recommended). Despite that, there are no plans to pursue such a policy at this time.

Review of PIA Policy/Legislation

A Canada-wide task force on identity management and authentification (IMA) is underway in the Summer of 2007. It is formed of representatives of government offices responsible for service delivery, some of whom are also under the same ministries as the CIO. While the report was not yet public at time of writing, one early recommendation is that PIAs be conducted for all service delivery projects, particularly those delivered electronically. There is a sub-committee looking at the need for a pan-Canadian PIA tool specific to IMA.

Lessons Learned

Utility of PIAs in Alberta

The Commissioner's message in his 2005/6 Annual report[76] groups his office's review of PIAs with "requests for information and comments on programmes and schemes". Together, the office's "involvement with public bodies in developing and refining programmes which collect, use and disclose the personal information of Albertans is important. This kind of collaboration pays big dividends in terms of developing sound programmes to serve Albertans, while using their personal information reasonably."

Regarding Health Information PIAs,

> "The HIA team has continued to focus efforts in overseeing steps taken by custodians to implement reasonable safeguards to protect health information in electronic health record systems. Privacy impact assessments continue to be an effective tool in assisting custodian's efforts to reasonably safeguard health information. The Commissioner received 353 PIAs this year, a 63% increase from the 217 PIAs received the previous year."[77]

The Commissioner feels that "fifty percent" of the value of the PIA is that it causes project proponents to look at things that they ordinarily would not. When organisations look at information collection, use and disclosure, rather than their usual perspective of achievement of organisational goals, they will see issues themselves.[78]

[76] Office of the Information and Privacy Commissioner, Annual Report 2005-6, Commissioner's message at page 2 at http://www.oipc.ab.ca/ims/client/upload/OIPC_AR2005-2006_web.pdf

[77] Office of the Information and Privacy Commissioner, Annual Report, 2004/5 – Table 1 at page 12 at http://www.oipc.ab.ca/ims/client/upload/OIPC_AR05.pdf

[78] Interview with Franklin J. Work, Q.C., Information and Privacy Commissioner of Alberta, Canada.

One way in which the mandatory requirement under the HIA for PIAs to be completed is “enforced” is through a joint programme of Alberta Health & Wellness, the Alberta Medical Association and Alberta's Regional Health Authorities. The fact that the Physician Office System Program subsidises health information systems and ties those funds to the completion of a PIA acts in favour of compliance with the HIA’s PIA requirements[79]. In addition to funding, the programme offers direct assistance in completing the PIA and produces a *Health Information Act Guide to Privacy Impact Assessments for Physician Offices*. It publishes a question and answer and provides other useful information on the process on its website. This prescriptive programme also requries a post-implementation review six months after implementation.

Another factor in enhancing compliance and quality of PIAs is the development of PIA expertise in vendors of health information software to health information custodians. These companies often bundle their wares and services to include assistance with the conduct of the PIA. Thus, these consultants acquire experience and expertise as they move from organisation to organisation, beyond that which any smaller organisation could hope to achieve. The Commissioner reports that these consultants follow the template and generally do an adequate job on the PIA, and that their participation in helping the smaller clinics in particular is appreciated by his Office.

The Commissioner reported an instance where a clinic that had conducted a PIA was broken into and computer equipment stolen. A privacy breach was averted because a software vendor assisting with completion of the PIA had recommended saving data to a secure, remote server to mitigate such a risk. While the clinic did not fully understand the risk at the time, it adopted the recommendation of the consultant.

The Commissioner commented publicly on the utility of PIAs in a media release.

> “The Information and Privacy Commissioner is pleased that the Alberta Cancer Board completed a comprehensive Privacy Impact Assessment prior to launching the [Alberta Web Surgical Medical Record] system. “I am very encouraged to see a Privacy Impact Assessment which means the Board is serious about protecting patient privacy. I have been talking about the need for Privacy Impact Assessments for quite some time, and I think other agencies and public bodies can learn from this”, said the Commissioner. “This is the kind of patient benefit we want from electronic information systems. By doing the Privacy Impact Assessment, we believe the Alberta Cancer Board has proven the need for the program and has taken reasonable steps to address privacy and security issues.”
>
> The Privacy Impact Assessment was submitted to the Office of the Information and Privacy Commissioner for review, and Work likes the cooperative approach. “We were able to review all of the privacy measures of this new system, check to see whether custodians are using the least amount of health information needed, whether users of the information will gain access on a need to know basis and whether information security is in place. In this case we are satisfied the Board took proper privacy measures”.[80]

The Director of a large Alberta government privacy office cites two instances where planned initiatives were assessed – one successfully enhancing the privacy of a proposed initiative, and one where the assessment did not foresee the media and public resistance that followed implementation. Both cases are highly instructive.

[79] Under the Physician Office System Program of Alberta Health, described at http://www.posp.ab.ca/. The privacy requirements are described at http://www.posp.ab.ca/implementing/privacy-impact-assessment-faqs.asp

[80] Canada Health Reference Guide, Commissioner applauds Privacy Impact Assessment of Alberta Cancer Board, Thursday, August 16, 2007, at http://www.chrgonline.com/news_detail.asp?ID=72227

Firstly, the Alberta government's central personnel agency proposed to do background checks on people it was considering placing in senior positions, to assess the risk associated with their hiring. Initially, full credit bureau, Canadian Security Intelligence Service (CSIS) and criminal record checks were proposed. Due to consultation with the Commissioner's Office, the responsible agency scaled back considerably on all fronts and limited the information collected and its distribution, while still being able to manage the risk they sought to address.

Secondly, there is an example of where a programme didn't go through a sufficiently comprehensive privacy assessment, and the result was a public outcry. This case involved an incremental change to an existing programme of publicising special needs children in need of adoption in order to increase the number of placements. The adoption programme had previously been advertising "Wednesday's Child" (a featured child of the week) on television regarding the child's need of adoptive parents with special skills. The initiative moved this information to the internet. A photograph and limited information about each child's needs was posted.

As a result of the initial screening, a "Privacy Scan" (short form privacy assessment) was done for this change in media of disclosure, instead of the full-blown PIA. Both the department's privacy office and Commissioner's office had been consulted. No one anticipated the opposition and concern about the privacy rights of the children.[81] When the site was launched in February, 2003, the media carried stories with headlines such as "Beware e-adoptions - Will clicking on a government Web site turn children into commodities?[82]", and "Calls for Alberta to shut down Internet adoptions".[83] "Opposition MLAs were foaming at the mouth in their condemnation of the province's adoption Web site. Posting photos and personal information about foster kids who need permanent homes is humiliating, hurtful and exploitive, they suggested.…The commissioner initially expressed concern that there was too much personal information on the adoption Web site, and Children's Services revised the site accordingly."[84] Ironically, as a result of the publicity, the number of adoptions and families attending an orientation session increased dramatically.

Room for Improvement

Oversight Body

Even with the HIA making PIAs compulsory for certain types of initiatives undertaken by health information custodians, the Commissioner does not feel his office receives as many as it would, were PIAs conducted in all instances in which they should be and sent to his office for review. However, as larger health organisations have privacy staff, he does think that his office sees PIAs for the larger, more complex system and instances of PIAs not being conducted when they should be likely arise in small organisations like doctor's offices and clinics, where the impact or reach is smaller.

The Commissioner also suspects that his office may only receive about 75% of the PIAs that should be done under the FOIP Act.

[81] To learn more about what information is currently available on-line see Alberta Children's Services Adoption Profile Lookup at https://www.child.gov.ab.ca/whatwedo/adoption/profilelookup.cfm

[82] Arthur Schafer, Globe and Mail, Beware e-adoptions - Will clicking on a government Web site turn children into commodities?, Friday, February 14, 2003 – Print Edition, age A19

[83] CBC News, *Calls for Alberta to shut down Internet adoptions*, Last Updated: Thursday, February 13, 2003 at http://www.cbc.ca/news/story/2003/02/12/adoptions030212.html

[84] Mindelle Jacobs, *Adoption Web Site is a Huge Success*, The Edmonton Sun, May 07, 1999.

Central Agency

According to the central agency, PIAs may not be completed in every instance that they should. They have heard that practitioners find them expensive (if paying a contractor) or simply a drain of internal resources.

Feedback from practitioners about the PIA process is that doing a PIA takes time and resources away from the primary business of the organisation and the process is overly complex.

Practitioners

According to the Commissioner, practitioners have provided feedback that the form is too long and not user-friendly. However, the Commissioner feels that the information requested is required. Some practitioners have difficulty answering particular questions, given the particulars of their initiatives, but Commissioner's staff members will provide guidance.

Research

The following individuals were interviewed:

Office of the Information and Privacy Commissioner (the oversight body):

- Franklin J. Work, Q.C., Information & Privacy Commissioner
- LeRoy Brower, HIA Director

Service Alberta (the central agency):

- Tom Thackeray, ADM, Information Services Service Alberta
- Hilary Lynas, Director, Access, Privacy and Security

Practitioner/Privacy Office:

- George Alvarez, Director, Information and Privacy Office, Alberta Employment, Immigration and Industry (providing privacy services to four other personal-information-intensive departments and agencies within the Alberta provincial government, including Children's Services, Advanced Education and Technology, and to the central government personnel agency.)

In addition, documents provided by these individuals and found on websites were reviewed. These included:

- PIA templates and instructions
- Web pages describing the PIA process
- Annual Reports
- Internet searches of media coverage of incidents cited by interviewees.

Appendix 1
Policy Regarding Privacy Impact Assessments
Alberta, Canada

The Alberta Government's central agency policy

Service Alberta's PIA Guidelines and Practices, Chapter 9, Privacy Compliance, *Privacy Impact Assessments*. This contains a good description of the PIA process and tools (reprinted below in its entirety, and available on-line at http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3)

9.3 Privacy Impact Assessments

A *privacy impact assessment* (PIA) is a process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy. The process is designed to ensure that the public body evaluates the project or initiative for technical compliance with the *FOIP Act* and also assesses the broader privacy implications for individuals. A PIA is both a due diligence exercise and a risk management tool. Although only real breaches of privacy contravene the privacy provisions of the *FOIP Act*, even the perception that privacy may not be adequately protected can seriously damage the reputation of a public body as well as the public's confidence in a particular program or initiative.

The PIA process requires a thorough analysis of the potential impact of the initiative on privacy and a consideration of measures to mitigate or eliminate any negative impact. The PIA is an exercise in which the public body identifies and addresses potential privacy risks that may occur in the course of its operations. While PIAs are focused on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy and security policies and procedures, or the lack of them, can be significant factors in the ability of the public body to ensure that privacy protection measures are available for specific projects.

A PIA provides documented assurance to the public body, to the Commissioner and to the public that all privacy issues related to the initiative have been appropriately identified and addressed. Once the Office of the Information and Privacy Commissioner is satisfied that the public body has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner or a staff member will accept the PIA. Acceptance is not approval. It merely reflects that office's acceptance that the organization has made reasonable efforts to protect privacy.

When is a privacy impact assessment needed?

Public bodies that are custodians and therefore subject to the *Health Information Act* for health information in their custody or under their control, should note that there are express requirements under the *Health Information Act* to conduct privacy impact assessments in certain situations (sections 46, 64, 70 and 71). Some of the public bodies under the *FOIP Act* that are affected by those requirements are regional health authorities, the department and Minister of Alberta Health and Wellness, the Alberta Mental Health Board and the Alberta Cancer Board.

Privacy impact assessments are not mandatory under the *FOIP Act* but are recommended for major projects that involve the collection, use or disclosure of personal information. **Section 53(1)(f)** of the *FOIP Act* provides authority for the Commissioner to comment on the implications for freedom of information or for protection of privacy of proposed legislative schemes or programs of public bodies.

Public bodies should consider conducting a PIA when

- new data elements will be collected and added to an existing personal information database, or a new database is proposed;
- system access will be rolled out beyond current parameters, controls, levels or numbers of users;
- the use of personal information will be expanded to include data linkage or matching or other purposes;

- limited disclosure or reporting about selected individuals will be expanded to enable broad disclosure of information about a larger population base;
- the way in which the system is accessed, managed or secured from a technical or managerial perspective is changed significantly (including use of internet technology or outsourcing); or
- the retention period for personal information in the system will be changed.

As information systems become more complex, the probability of having an unexpected impact on privacy increases. Initiatives that appear to involve minor technical enhancements for client convenience and public body efficiency may significantly impact individual privacy.

The Privacy Policy and Assessment Unit of the Office of the Corporate Chief Information Officer, Government of Alberta, is responsible for ensuring that government information and communications technology (ICT) projects, especially cross-government projects, comply with all applicable privacy legislation. The Unit coordinates policy development, privacy impact assessment procedures and privacy architecture development for ICT in the Government of Alberta.

What is the process for a PIA?

Consider establishing a PIA development team

Determine which staff can best provide the information that is needed for the PIA. The team could include the FOIP Coordinator, the project or program sponsor, records manager, project manager, IT/IM specialists, legal services, communications specialist and a senior or executive manager.

Identify someone to lead the process and write the PIA. Ideally, this would be someone who understands the *FOIP Act* and privacy principles and issues, has technical writing skills, has project management experience and can synthesize input from a variety of sources.

Public body FOIP Coordinators play a role in the preparation and routing of PIA documents. Provincial government department FOIP Coordinators should note that, if an information technology system or enhancement involves more than one government department, the Office of the Corporate Chief Information Officer of the Government of Alberta should be consulted in the preparation of the PIA.

Consider when to start the process

If the PIA is viewed as an obstacle to the initiative being launched, it has been started too late. If decisions about the initiative are not firm, resources have not been committed and questions about privacy implications cannot be answered, it is too early to start the process.

The Office of the Information and Privacy Commissioner believes that a PIA is rarely ever finished. It is a dynamic document that should be updated from time to time as changes are contemplated for the program. Public bodies are expected to advise the Commissioner's Office of any changes or modifications to the program and to provide documentation so that the PIA on file is always up to date.

Determine who will approve the PIA internally

The internal approval of a PIA should be based on the public body's established internal approval process and should include approval from the members of the PIA development team.

Consider whether public consultation is needed

It may be appropriate to consult with stakeholders or with a larger public audience on major initiatives or on significant overhauls of existing programs. Focused public discussion conducted early in the process can help program or system designers anticipate public reaction to proposals or help to eliminate options that meet with significant resistance. The public body should address in the PIA how it intends to educate and consult with affected stakeholders respecting the proposed initiative. Alternatively, the justification for not consulting should be set out in the PIA.

Understand the role of the Office of the Information and Privacy Commissioner

To give the Commissioner's Office time to formally review and comment, public bodies should provide the PIA to the Office at least 45 working days before implementing the proposed new or changed practice or system. In practice, however, the role of the Commissioner's Office starts long before the formal review. The process for interaction with the Commissioner's Office is as follows:

- The public body (usually the FOIP Coordinator) advises the Commissioner's Office of the project to be undertaken, well in advance of implementation.
- If necessary, the PIA development team meets with the staff of the Commissioner's Office to review the project and determine whether a PIA is required. The Commissioner's Office decides whether a PIA is required and requests the public body to conduct one.
- If a PIA is required, it must be submitted to the Commissioner by the head of the public body .
- The PIA development team prepares the PIA by completing the PIA Questionnaire (published by the Office of the Information and Privacy Commissioner), with the necessary elaboration and enclosures and submits it (through the head) to the Commissioner. The FOIP Coordinator may send a working copy of the document to the staff of the Commissioner's Office prior to the head's submission.
- Questionnaire responses are reviewed by the Commissioner's Office and discussed with the PIA development team or its leader, as required. Further information may be requested, which could result in an extension to the optimal 30-day review period.
- Upon final acceptance by the Commissioner's Office, the head of the public body receives a letter of acceptance from the Commissioner. This letter also advises of any future activity by the Commissioner's Office.
- The PIA is filed in the library of the Commissioner's Office and is available for public review. Public access to some confidential information, such as details of sensitive security measures, is sometimes restricted. Any such restrictions are limited and specific.
- The public body provides updates to the PIA as changes to the project are implemented over time.

The Commissioner's Office may use the PIA as a starting point for any investigation into a breach of privacy.

The Office of the Information and Privacy Commissioner publishes a document on the PIA process called *Privacy Impact Assessment: Instructions and Annotated Questionnaire*. The Office also publishes a *Privacy Impact Assessment: Supplementary Organization Questionnaire* that is intended for use in projects involving more than one organization. These packages are available from the Commissioner's web site at www.oipc.ab.ca, or by requesting a PIA package by from the Office ((780) 422-6860; or toll free 1-888-878-4044).

Privacy impact assessment questionnaire

The PIA Questionnaire will be considered a public document by the Office of the Information and Privacy Commissioner. Any appendices or attachments will also be considered public documents unless they are explicitly designated as confidential. Examples of appendices would be an organizational strategic or business plan addressing privacy protection or physical or information security plans and access control documentation. Appendices that are designated as confidential must be accompanied by the reasons for the confidentiality.

The PIA Questionnaire must be submitted to the Commissioner with a covering letter from the head of the public body in order to receive a formal response.

For public bodies that are also custodians under the *Health Information Act*, there are statutory requirements for privacy impact assessments in sections 46, 64, 70, and 71 of that Act that must be complied with. Those bodies may use the same PIA Questionnaire for conducting a PIA under the *Health Information Act* with a few modifications. (For more information on conducting PIAs for purposes of the *Health Information Act*, see Chapter 5.2.8 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness.)

The questionnaire is divided into two parts:

- Part A: Organizational Privacy Management; and
- Part B: Project Privacy Management.

Each part contains a series of questions. The checkboxes on the questionnaire provide for summary responses to the questions. The note fields provide for elaboration of the responses, as necessary. There is also a column that can be used to cross-reference separate enclosures. The questionnaire can be completed either in paper or electronic formats.

Part A: Organizational Privacy Management

This part of the questionnaire is intended to provide background on facets of privacy management across the public body which may affect the management of privacy issues for the specific project. If this information has been provided with a previous PIA and has not changed, it does not have to be resubmitted. One set of questions in Part A is designed to provide information, including documentation if available, from the public body about its privacy protection policies, controls and procedures. This would include such things as a privacy charter, policy or strategic plans relating to privacy protection and any procedures that have been developed related to information security, records management, waste management, need to know, etc. The second set of questions deals with the structure and organization for dealing with security and privacy protection within the public body. This would include information on whether a position in the organization has been designated as responsible for privacy and security; the management reporting process for dealing with privacy compliance issues and training of new staff in privacy protection.

Part B: Project Privacy Management

In this part of the questionnaire, the public body provides information specific to the proposed project. The information requested includes

- a project description, including a listing of data elements to be collected, used or disclosed; an information flow diagram; and a listing of who will have access to the information;
- an analysis of the proposed information flows in relation to the rules in the governing privacy or other legislation regarding collection, use, disclosure, protection, accuracy, retention and disposition of personal information;
- a privacy risk assessment in which the public body identifies the potential privacy risks of the project and shows whether those risks have been successfully addressed through system design or policy measures or through other proposed options for mitigation. The residual risks that cannot be addressed through the proposed options should also be identified. Where possible, the likely implications of those risks in terms of public reaction and project success should be analyzed;
- a description and relevant documentation related to the privacy controls and security measures or procedures for the specific project; and
- the arrangements that have been made for audit, compliance and enforcement mechanisms for the proposed project, including information about how audits would be conducted and how any identified privacy issues would be addressed.

When the development of personal information systems is contracted out, the need to develop privacy impact assessments should be among the privacy requirements included in any management or operations contract governing the project and should be identified in the Request for Proposals or Tender documentation.

IV. BRITISH COLUMBIA PROVINCIAL GOVERNMENT

Context

British Columbia is one of 10 provinces in Canada and is the 3rd most populated at a quarter million residents of Canada's 32 and a quarter. "More than two-thirds of British Columbia's population is concentrated in the Lower Mainland [which includes the major commercial city, Vancouver] and [adjacent] southern Vancouver Island [which includes the capital city of Victoria]."[85]

BC has long been a front-runner in privacy legislation, and it is in the process of a major review and revision of its PIA tool and process which may be very instructive.

Legislative and Policy Framework

Legislation

The applicable public sector privacy legislation governing Privacy Impact Assessments (PIAs) in British Columbia (BC) is the *Freedom of Information and Protection of Privacy Act,* (FOIPPA), RSBC 1996, c. 165.[86] This legislation was proclaimed in 1992, became effective for ministries in 1993, for local public bodies in November of 1994 and Governing Bodies of Professions or Occupations (Schedule 3) in November 1995.

FOIPPA applies to all government ministries and named closely-held public sector organisations, collectively called "public bodies" (listed in Schedule 2 of the Act and amended by Regulation). While BC also has privacy legislation governing *private* sector organisations (the *Personal Information Protection Act*, [SBC 2003] Chapter 63), it is not as specific regarding processes and administration, and does not address PIAs.

As of April, 2002, section 69(5) of FOIPPA requires ministries to conduct PIAs for "a new enactment, system, project or program" (hereafter collectively referred to as "initiative")[87], *to determine their compliance with Part 3 of FOIPPA* (which governs the collection, use, disclosure, protection and retention of personal information by public bodies), in accordance with direction provided by the minister responsible for the Act. This provision gives the Minister with the authority to develop mandatory policy with regard to PIAs for ministries, but it does not apply to all public sector organisations subject to the Act. However, under s. 69(7), the Minister may require any of the other public bodies which are subject to the FOIPPA to comply with PIA policy as if they were ministries, but this has never been exercised.

There are mandatory, periodic, legislative reviews of FOIPPA, the latest of which was 2004. Members of the public, organisations subject to the Act and invited experts may testify and submit briefs to a multi-party committee of the Legislative Assembly. The Minister responsible usually introduces some amendments following a review, but is not obligated to follow the Committee's recommendations. The Minister can introduce amendments at any time with Cabinet approval, and can also make policy changes at any time.

[85] Statistics Canada at: http://geodepot.statcan.ca/Diss/Highlights/Page9/Page9c_e.cfm
[86] Find FOIPPA at: http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm.
[87] Under FOIPPA s. 69(1) definitions, **"privacy impact assessment"** means an assessment that is conducted to determine if a new enactment, system, project or program meets the requirements of Part 3 of this Act.

Policy

The Minister has developed PIA policy, and it is contained in the Information Management and Information Technology chapter of a government administrative policy and procedures manual, and will be augmented by a policy supplement specific to information policy (forthcoming). The central agency responsible for government privacy policy is the Information Management/Information Technology Privacy and Legislation Branch (hereafter referred to as "the central agency") in the Office of the Chief Information Officer within the Ministry of Labour and Citizens' Services.[88]

This body of policy requires ministries to complete PIAs for all initiatives in a prescribed format, and to *submit* completed PIAs for review by the central agency for certain types of higher-risk and profile initiatives (as described later under Review/Approval of PIAs).

Cabinet Operations also requires PIA's to be prepared for legislative proposals that involve personal information.

The British Columbia PIA Process

As of early autumn, 2007, British Columbia is nearing completion of a fairly comprehensive review and revision of its PIA process, tool and guidance material. Its methodology, findings and new PIA direction are described in a later section. The following describes the current process and tool which have been in place since early this millennium.

The Tool

The central agency publishes two standard tools for the conduct of PIAs:

1. Privacy Impact Assessment [PIA] Process[89]
   This is also found in the Chapter 12, Information Management and Information Technology Management chapter of the Core Policy and Procedures Manual published by the Office of the Comptroller General.[90]
2. Privacy Impact Assessment (PIA) Template[91]
   This is essentially a form and a checklist for implementing the PIA Process and determining whether the requirements of the legislation are met by the new initiative.

The PIA Template is a compliance checklist. It is organised in the same way as the legislation, with parts on collection, use, disclosure and security of personal information and questions relating to most of the sections (except administrative ones) of the Act. It is web-based, printable and can be saved and modified.

The yes/no answers are *not* augmented throughout most of the form with space to explain. For example, under Collection of Personal Information, there are ten yes/no questions about the authority to collect.

In addition to the checklist, the PIA template requires a personal information flow chart, and other information about the initiative is often copied in from other planning documents or appended.

[88] See http://www.lcs.gov.bc.ca/CIMB/ for this central agency's website.
[89] At: at: http://www.lcs.gov.bc.ca/privacyaccess/PIA/PIAprocess.htm.
[90] At: http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm.
[91] At: http://www.mser.gov.bc.ca/privacyaccess/PIA/PiaTemplateRevisedMay06.doc.

The Background section to the PIA process overview states with typeface emphasis that, "In all government initiatives, privacy protection should be seen as a design objective, not an obstacle to overcome."[92]

The PIA process overview describes the PIA as follows. "A Privacy Impact Assessment (PIA) is a foundation tool/process designed to ensure compliance with government's privacy protection responsibilities and is a requirement under section 69(5) of the FOIPP Act. The PIA is intended to support government business objectives, including electronic government initiatives. If used as part of normal business processes, the PIA can ensure that privacy requirements are identified and satisfied in a timely and cost efficient manner. The PIA can make the difference between a privacy invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs. The PIA process is also designed as an educational tool, since participation in privacy impact assessments promotes privacy awareness."

The overview further states that the "new" version is supposed to be simpler to use, "allowing for much of the assessment to be done by those most familiar with the business or product being assessed", and "appendices of special assessments, such as for systems initiatives, where data flow analysis may be important to understanding the use of personal information".

A government-wide review of the PIA form is being led by the central agency. As of the Autumn of 2007, the revisions arising from this review are still in progress, but research had been completed, direction set and rewriting is well-underway. This review and revision of the PIA template is discussed in the next section, BC's PIA Review and Revision.

Completion of PIAs

By Whom?

The PIA form is designed to be completed largely by programme staff. Certain sections of the form are to be completed in consultation with the Director or Manager of Information and Privacy (DMIP). Other sections, such as those relating to information system security, must be completed by the area responsible for IT systems.

In practice, the process for completing PIAs differs by ministry. In some cases ministry information and privacy office staff or head completes the PIA with information provided by programme staff.

"Ministry Directors/Managers of Information and Privacy are responsible for ensuring that the collection, use and disclosure of the personal information in ministry custody or under ministry control, including personal information that is in the custody of arms length service providers or contractors, is in accordance with [FOIPPA]."[93] Therefore, they are responsible for ensuring that PIAs are conducted even when the public body itself is not handling the personal information.

A recent development is a trend toward having IT contractors involved in developing systems complete the PIA form.

[92] *Privacy Impact Assessment [PIA] Process,* Ministry of Labour and Consumer Services, at: http://www.lcs.gov.bc.ca/privacyaccess/PIA/PIAprocess.htm.

[93] Information and Technology Management Manual, Supplement to Chapter 12, Core Policy and Procedures Manual, 12.3.2 II f., *Privacy Impact Assessments (PIAs*), Ministry of Management Services, Release 1.1.3, September, 2004, at http://www.cio.gov.bc.ca/prgs/CPM12.pdf.

Central government policy explains the role of the central agency in PIAs:

> **"The Information Policy and Privacy Branch (IPPB)** is responsible for providing advice and assistance to ministries undertaking PIAs, where needed, and for a final review where personal information is collected, used or disclosed. Where required, IPPB may also conduct PIAs on corporate or cross-government initiatives. A corporate system is defined as a system that more than one ministry directly accesses for the purposes of inputting or correcting data/information." [94]

When?

According to central government policy, ministry programme managers "are responsible for ensuring that a Privacy Impact Assessment is completed during the *early development stages* of a program, legislation, system or other initiative as a component of the project or business plan."[95]

Even when organisations determine that there is no personal information being collected, used or disclosed, they are expected to document this determination by completing Section 1 of the PIA, Basic Information. In this case, sign-off is not required. Part 1 requires information on the organisation, contact information, a description of the initiative being assessed, Purpose/Objectives of the initiative, potential impacts, details of any previous PIA or other form of personal information assessment completed. Practitioners are to note under the description of the initiative if the initiative does *not* collect, use or disclose personal information. Programme staff are allowed to make that determination without consulting with privacy staff.

This appears to create the potential for PIAs not to be completed when they should be if, for example, the personal information is in an unusual form not recognised as such, or if the initiative is not yet sufficiently developed for those completing the PIA to be aware that it will entail collection, use or disclosure of personal information.

BC's PIA process overview states in emphasised text that "It is important that a PIA be completed during the early developmental stages of any program, system or other initiative as a component of the project/business plan", which underscores the risk that the initiative will evolve to involve personal information after the PIA is completed. There is no mention of follow-up PIAs for later stages although it is anticipated that these will be done.

External Consultation

The only guidance provided in the PIA template and overview regarding consultation is to consult *internally* with privacy or records management experts, or information systems staff where appropriate. Consultation with *external* groups such as clients or public interest groups is not generally mentioned in PIAs or discussions about PIAs.

Even though the revised PIA has been designed with a view to being completed, at least in part, by programme staff, there are a number of questions in the PIA where consultations with privacy experts are recommended if not required. On the template, these questions have been designated with an asterisk in the margin.

In practice, public bodies often consult on the privacy implications of their initiatives with the Office of the Privacy Commissioner on the initiative, but this is not always in the context of the PIA, and a PIA may or may not be shared. The Privacy Commissioner is

[94] Ibid.

[95] Ibid.

an independent officer of the legislative assembly and not part of government, and has an oversight role with regard to all privacy legislation.

Review/Approval of PIAs

Internal

PIAs must be signed off within the ministry by the ministry Director or Manager of Information and Privacy (DMIP) and senior executive. In addition to DMIP review, certain parts must be reviewed by other specialists like information technology departments for information systems and records managers. The PIA contains a section with signature blocks to ensure that these signatures are obtained.

Central Agency Review

By policy, ministries must submit certain types of PIAs to the privacy central agency for review. The initiatives which must be submitted for review include:

- Alternative service delivery and outsourcing projects
- Corporate systems (cross-government, whether automated or not)
- Information-sharing and data linkage agreements
- Legislative proposals

The central agency reviews the PIA and may seek additional information from the PIA sponsor, may discuss alternatives and provide advice, but does not "approve" PIAs. It issues a letter to the ministry stating that the initiative is compliant with FOIPPA or expressing unresolved concerns.

The central agency also occasionally receives PIAs from public bodies which are not required to submit them, and from ministries where the initiative is not of the type for which a PIA must be submitted. The central agency reviews all of these and treats them like the mandatory ones.

Four or five central agency staff members are involved in reviews of PIAs, among other duties. Very often, there is a good deal of interaction with sponsor staff, including requests for clarification or further information or suggestions from central agency staff. Review can take a couple of days for simple initiatives where the information is complete and when workload is light, to several months where there are a number of issues to be resolved and more than one organisation is involved in the initiative.

Ministries often make revisions to the PIA and changes to the initiative as a result of input. Resistance is greater if the process of developing the PIA is started late in the initiative's lifecycle. However, most suggestions are well-taken.

Oversight Office Review

There is no requirement for the Office of Information and Privacy Commissioner (OIPC) to review or approve PIAs. However, ministries often decide, of their own volition, to consult the Office of the Information and Privacy Commissioner on the privacy implications of their initiatives, either with or without a completed PIA in hand. Whether or not a PIA has been provided, the OIPC often finds that it needs a meeting with ministry staff to determine what the new initiative actually does with personal information, at a more detailed level than is usually supplied.

Every time the Office is formally asked for assistance, it opens a file. According to the Commissioner's 2006/7 Annual Report, it opened nine of this type of file initiated by public bodies or organisations, two the previous year and seven the year prior.[96] According to the narrative, "public bodies and private organisations frequently ask us for advice on privacy/access implications of proposed policies or current issues and may ask us to review privacy impact assessments they have prepared for proposed policies or programs."[97]

The motivation of ministries voluntarily consulting the OIPC comes from the Commissioner's legislative authority, under s. 42(1)(f) to comment publicly on privacy implications of initiatives.[98] The fact that government would prefer to avoid such public comment is a key motivator in improving the privacy aspects of their initiatives.

In agreeing to consult, the OIPC makes it clear that it reserves the right to comment on the initiative in future and that its input does not guarantee favourable rulings, should a case ever arise regarding the subject of the PIA. During consultations, the OIPC is primarily concerned about whether the new initiative will comply with FOIPPA, but also tries to be helpful in providing ideas about how goals could be achieved in less privacy invasive ways.

External Review

PIAs are not subject to external review in BC.

Public Availability

PIAs are not, as a rule, proactively released or readily available on-line. However, interested parties can access a list of PIAs conducted to determine if there is a PIA they would like to request under Freedom of Information legislation. The types of information that may be subject to severing could relate to the security measures for information systems or plans going to Cabinet for consideration and not yet public.

Sections 69(2) and (3) of FOIPPA requires the Minister responsible for the Act to maintain and publish a Personal Information Directory (PID) that contains, among other items, *any privacy impact assessments a ministry has conducted*, and any other information considered appropriate. This directory was established as a result of the April 2002 amendments and is the first of its kind in Canada.[99] A searchable utility for the Personal Information Directory (in which PIAs conducted must be listed) is available on-line.[100] Each listing provides a title and, in some cases, comprises one or two sentence summary of the initiative for which a PIA has been conducted. Ministries are responsible for the content and posting of their own PIA summaries, although the database is maintained centrally.

[96] Office of the Information and Privacy Commissioner for British Columbia, 2006-7 Annual Report, Table 1. FIPPA and PIPA Files Received and Closed, April 2006 – 31 March 2007, p. 10.
[97] Ibid., page 11.
[98] FOIPPA s. 42 (1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may …. (f) comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs of public bodies.
[99] From *Enhancing the Province's Public Sector Access and Privacy Law*, Special Committee to Review the Freedom of Information and Protection of Privacy Act, p. 43, at: http://www.oipcbc.org/pdfs/public/Rpt-FOIPPA37-5.pdf.
[100] BC's Personal Information Directory containing PIA summaries is at http://www.mser.gov.bc.ca/foipid/public/query.asp?FreeText=on.

Despite being called a “summary”, the information in the PID on the PIA only names the initiative that is the subject of the PIA, gives a little contact information and records management information. The summary of the initiative is one or two sentences but there is no information on the results of the PIA. The date the PIA was completed in entered, but not the posting date, so it is not possible to gauge how current the PID listings are.

Currently, 147 PIA summaries are listed on the Directory, from 2002 onward. This appears to be well short of the number of qualifying initiatives. Some ministries have informally confirmed that not all PIAs completed are currently listed in the Directory, and that this is largely a matter of priorities for resource or timing issues.

As part of this research, several ministries were contacted to ask for or about the process for obtaining full Privacy Impact Assessment reports, to test what they had been told about the process for public access and the accuracy of information in the Directory. It was difficult and time-consuming to find a person who knew about the process for obtaining reports using the contact information in the Directory.

BC’s PIA Review and Revision

Background

British Columbia’s PIA process, introduced in 1998, has undergone a major revision at the turn of this decade, resulting in the current version. The first PIA tool was narrative in format, based on the structure of FOIPPA. Practitioners were instructed to describe their initiative’s plans for collection, use, security and disclosure of personal information. Feedback about the amount of work required led to development of the current comprehensive checklist format. The PIA template is again under review in 2007.

The "Privacy Impact Assessment Form Redesign Project" began with preliminary research in Autumn of 2006, and received formal approval from the Government’s Chief Information Officer in January 2007. The Project is led by the central agency. Its purpose is: "To develop a corporate privacy impact assessment (PIA) template that addresses privacy requirements under the *Freedom of Information and Protection of Privacy Act* (FOIPP Act), while maximizing the PIA's usefulness and ease of use."

High level deliverables are:

1. Background review and examination of PIAs used in other jurisdictions;
2. Liaison with stakeholders about the current template and what they would like to see in a redesigned template, through a survey and a continuous improvement initiative;
3. Development and evaluation of a process map showing the steps to complete a PIA form;
4. Research and design of questions / modules / tips, as determined, to obtain information to populate the form;
5. Redesigned template, with possible option to be completed on paper or electronically; and
6. Ministry training on use of new template.

The project is currently addressing item 5, Redesign, which it hopes to complete by the end of the calendar year, with approvals being obtained early in 2008.

Impetus for the Review

Complaints about the template had been heard from many camps, and reviewing the process had been a task that the Council of Directors and Managers of Information and Privacy (DMIP Council) had wanted to tackle for some time.[101]

The current checklist was not as simple as practitioners wanted, and required programme staff who might not be familiar with privacy principles and legislation to make judgments about the compliance of their plans with the legislation. In addition, regulators reviewing completed PIAs found that they often did not have enough information to understand the initiative's personal information practices and make their own judgments.

Method and Project Structure

The central agency's Manager of Legislation & Privacy Policy headed the PIA Form Redesign Project. To form the PIA Review Committee, DMIP Council was asked to nominate representatives, and a committee of five members was formed which included two DMIPs and two working level members of other ministries' privacy staff. A representative from the Office of the Privacy Commissioner was also invited and participated at the start.

A survey was sent to ministries to solicit input on the PIA tool and process. The target audience included information technology and security staff, records management experts, and privacy staff. This was followed by a focus group.

To define the problem to be solved, a day-long professionally-facilitated focus group or collaborative session was held. Every ministry was invited to send a representative, preferably someone who had completed a PIA. Participants included representatives from ministry offices responsible for various information management functions (e.g., records management and information security), as well as practitioners who had completed PIAs. One of the first tasks was to describe what they didn't like about the current process and form. It took about an hour, and agreement was readily forthcoming. The deficiencies were prioritised and this became the basis for the problem definition for the project.

The Review Committee conducted a survey of PIAs in comparable jurisdictions, including the Canadian and provincial governments, the government of Australia and New Zealand and the USA's Department of Homeland Security. Results were compiled in tabular form and addressed such considerations as:

- Whether legislation addressing PIAs was in place,
- Whether PIAs were *required* by legislation or regulation,
- Whether there was a structured pre-assessment and assessment process,
- Whether there was a template,
- What content was covered and whether harm mitigation was addressed, and
- Whether there was a user guide and training in place.

Once revisions are complete, the new questions that will be pre-tested before they are computer-programmed.

[101] DMIP Council is a forum convened by the central agency with members consisting of the heads of privacy for each ministry and some other public bodies who wanted to participate. It meets approximately monthly, and discusses issues of common concern and often forms sub-committees to develop policy, reports and legislative proposals.

Findings

It was agreed that the current PIA tool and processes could be improved by provision of:

1. A better template, as it:
   - was confusing and contained unclear terminology for the lay people who completed it, as it was based on the structure and wording of the FOIPPA (privacy jargon, to them);
   - did not address mitigation of privacy risks or consideration of less privacy-invasive alternatives;
   - lacked narrative description that would allow privacy experts to review compliance determinations made by practitioners;
   - entailed inefficiencies, in that it somewhat duplicated other requirements for information systems development, and did not feed into the Personal Information Directory database where PIAs conducted are listed publicly; and
   - did not provide a means to electronically append supporting documentation or share electronically with others to collaborate on its development.
2. Better guidelines and advice on the process;
3. Training.

Direction of Change

In format, the new template will be in greater part narrative but still part checklist, with certain electronic enhancement including navigation and the ability to collaborate and route to others and to append other documentation. New structure and organisation will separate the tool from the statute and allow for multiple versions for different stages of development of the initiative.

The proposed PIA tool will be web based and interactive. "Yes/No" radio buttons will provide the user with direction, ensure all questions have been considered, and that sections that are not necessary for the type of initiative can be skipped.

It was determined that different types of initiatives have different requirements to assess privacy risks, and the current one-size-fits-all approach is not optimal. Therefore, BC is planning to develop separate PIA tools for:

- Legislative proposals;
- Information systems;
- Other types of new projects, programmes or initiatives; and
- Incremental changes to existing initiatives (except for legislative changes which will probably use the specific form even if only amendments).

The new tool will increase the amount of narrative description required. Programme staff will describe their initiative's plans, allowing privacy experts to pass judgment and suggest alternatives. This is seen as much preferable to a checklist where potential novices make judgments about compliance and personal information practices.

Other PIA Tools and Processes in British Columbia

Other public sector organisations that are subject to FOIPPA are not required to complete PIAs or follow government policy regarding them, but some, particularly in the health sector, have developed tools of their own.

BC has a system of primarily state-funded health care. The Ministry of Health has developed a template for PIAs conducted relating to the eHealth Initiative which is a multi-year, inter-jurisdictional programme to coordinate electronic delivery of health services by a variety of organisations.[102]

The eHealth PIA template, last updated April 2007, is in report outline with bullets to indicate what information should be covered in each section when it is completed in narrative form. As it is tailored for eHealth projects, it also has some specific elements associated with information systems development. It requires a system architecture diagram(s) and data flow map and a chart of data elements by data source and purpose and rationale for collection and use. It has a section for a Privacy Risk Analysis, which requires:

- Identification of privacy risks associated with personal information practices, including
  - consideration of potential benefits that may justify reduction of personal privacy;
  - what could happen if the system is not implemented, and
  - identification of groups would be most affected by the implementation of the system
- A strategy and/or measures taken to address or mitigate privacy issues, including identifying how identified privacy risks are mitigated and documentation of consideration of less privacy intrusive alternatives to what is being proposed
- Consultations with key stakeholders
- Strategy/communications plan to address public concerns
- Employee training plan

Responsibility for health care delivery is decentralised from the provincial government to regional Health Authorities. Health Authorities are public bodies under FOIPPA, meaning that they have to comply with the Act, but they are not subject to PIA policy. Therefore, some authorities have, on their own, developed a PIA tool specific to their needs. The recently revised Vancouver Coastal PIA template is based on the ten privacy principles of the 1995 Canadian Standards Association privacy standard, the *Model Code for the Protection of Personal Information* (Q830).

British Columbia PIA Training

The central agency offers general and specific PIA completion training sessions on a scheduled or dedicated basis on request. It is open to staff from ministries and public bodies. Classes are publicised by sending notes to all ministries and public bodies once a schedule is developed. Class size is limited to about 30 individuals, and a series of sessions are offered approximately twice a year. Courses are about a half-day in

[102] See http://www.health.gov.bc.ca/ehealth/ for more on the eHealth initiative and http://www.health.gov.bc.ca/library/publications/year/2005/ehealth_framework.pdf for the more detailed Framework document that lists specific projects and describes the privacy priority.

duration and are conducted by central agency staff experienced in the review of PIAs. The format is slide presentation and interaction and question and answers.

In addition, an introduction to PIAs that describes PIAs and their benefits, without addressing how to complete PIAs, is in the process of being developed for inclusion in a non-degree, professional development privacy course. The course will initially be a stand-alone introduction but is meant, in time, to be followed by more in-dept certificate based privacy training.

Lessons Learned

Utility of the PIA

Completion of the PIA may be the only time that staff involved in designing a new initiative look at it from a privacy perspective, and that has value. Central agency staff has learned of programmes making changes to the initiative as a result of questions considered in the PIA process. Changes are also often made in the course of review and questioning of the completed PIA by the central agency.

The greatest benefits are achieved when the PIA is conducted early enough in the process, and not when changes become more costly (particularly as in the case of information systems initiatives).

British Columbia's PIA overview is explicit that the PIA is viewed as a risk management tool with a specific focus on privacy. It plays a role in avoiding privacy 'harms' that non-compliance would entail.

There are definite benefits of having central privacy experts review PIAs completed by programme staff. Changes to the initiative are often made as a result of central agency input and suggestions. PIA sponsors are usually very receptive and seldom resist; under BC's FOIPPA, the legislature can pass non-compliant legislation "notwithstanding" the Act. By the end of a PIA review, the vast majority of reservations or concerns have been dealt with and the final letter gives the initiative a clean bill of privacy health.

An unintended benefit in having PIAs reviewed centrally is that initiatives from the far corners of government can benefit from a corporate perspective, sometimes unrelated to privacy or matters of privacy compliance. However, certainly, privacy considerations are the bulk of the central agency input and advice. This can take the form of informing the PIA sponsor of alternatives and technology that could be less privacy invasive, but does not go as far as telling the ministry what choice to make. It may also be a matter of being in touch with public opinion on privacy matters, and passing on a suspicion that once the plans or programme were made public, the initiative would be likely to meet with an outcry or resistance.

Since the privacy central agency is part of the central CIO's office, and closer to central government decision-making, its staff may be aware of similar initiatives already underway or planned, overlap between programmes, or inconsistencies with government's current or planned direction.

Room for Improvement

Much of the room for improvement uncovered in BC is discussed in detail above, under BC's PIA Review and Revision.

Oversight Body – the OIPC

According to OIPC staff, completed PIAs do not always provide a good understanding of the privacy aspects of an initiative. A meeting is usually needed to probe cursory information on the form, and supplemental documentation is often required. A meeting is found to be more useful and efficient use of OIPC time for the purpose of understanding the privacy implications of a proposed system or programme than review of a completed PIA.

OIPC staff also reports that those who complete the PIA form find that it is "a lot of work", and that the only benefit is to comply with policy and legislation. Therefore, the PIA product can be seen as a net drain of resources, with little benefit for creator or regulator.

Despite this, there are areas that a checklist form does not address, such as mitigation of privacy risks and problem-solving. The form also does not require consideration of access to personal information, a right provided by the legislation.

Ministries' interest in completing the form is to document compliance, and a checklist format allows them to do that, even if compliance is questionable. The form does not require practitioners to ask the "big questions" such as, "Should I be doing this?" and "What direction is this taking us, in the long term with regard to privacy?"

The core of the BC PIA is the required flow chart. However, a programme flow chart is usually provided, and not a personal information flow chart, which could be very useful. Arrows into the initiative would represent the collection of certain personal information, and each arrow out a disclosure. Within the programme, uses would be described. If each arrow were to have a corresponding detailed description of the data elements, means of providing consent or other authority for collection, agreements under which information is to be disclosed, etc., then this would provide the information that internal ministry privacy experts or regulators would need to understand the initiative and determine if there might be any compliance gaps.

OIPC staff believes that a PIA should not be a one-time event. A PIA of some type should be conducted at the conceptual stage of a initiative, again once it is better developed, and at the end, to ensure that what was planned was done and that the initiative is still compliant.

The OIPC feels that the PIA should be more interactive and instructive to the user, with cautions or alternatives being provided, depending on answers given. The OIPC agrees with the decision of the PIA Review Project to create PIA streams for different types of initiatives such as information systems and legislation.

Despite this, the OIPC agrees with certain decisions such as the intention of the PIA Review Project to create PIA streams for different types of initiatives such as information systems and legislation.

It is unlikely that one person can have sufficient programme and privacy knowledge to complete an entire PIA. Discrete sections to be completed by different experts would be beneficial.

Central Agency

A preferable format to the current checklist template would be one that requires programme staff to describe their PIA plans, but not to pass judgment as to compliance with privacy law. Privacy experts reviewing this narrative would be able to understand the planned initiative and make those judgments, as well as supply alternatives or question the need for privacy invasions. An example of how asking programme staff to make judgments on compliance could go wrong follows. If the person completing the form misinterprets a term such as “quasi-judicial tribunal” or “purpose of law enforcement” (terms which appear in the legislation), and tick the “yes” box, it may appear that the initiative has authority to collect personal information where it does not. Privacy laypeople may not be aware of the jurisprudence arising from the Commissioner’s rulings that have defined these terms over time. If those completing the PIA were required to name the “quasi-judicial tribunal”, etc., a knowledgeable reviewer might realise that the body did not meet the criteria and that therefore, the initiative was not authorised to do what it proposes with personal information.

According to the central agency, the current one-size-fits-all approach is not optimal, and specific templates tailored to the type of initiative could be more effective.

Practitioners

Prior to conducting its review and revision exercise, the central agency met with some users and received feedback on BC’s PIA form and process. Feedback from practitioners participating in the PIA Form Revision Project focus group is described in the section, BC’s PIA Review and Revision.

Ongoing feedback to both the oversight agency and central agency are that the process is much work without much benefit and confusing to someone not intimately acquainted with the legislation.

Case Study – When a PIA is not conducted

It is important that a PIA screening tool includes changes in the medium of disclosure of personal information as criteria for conducting a PIA. In one high-profile case in BC in 1996, the OIPC conducted an Investigation after the City of Victoria made property value assessments, by law, public information, available on its public website. The information had previously been made available in a variety of ways, but had never so readily accessible or searchable. Many people were taken aback by the media and public reaction to what seemed such an innocuous change in the means of disclosure. A privacy impact assessment, not required by policy or legislation, had not been conducted prior to making the change.

According to the investigation report, [103]

> “The new service would allow the public to search the database by property owner's name, address and Roll number. Further search would yield the location of the property, assessed values, actual values, legal description, current year tax levy and "other related information about the property." On the first day of operation, "Assessing OnLine" received more than fifteen thousand visitors--most of those local.[1] Until then, the City of Victoria had received an average of twenty-five to thirty calls per day inquiring about property assessments.
>
> The ensuing commotion focused attention on the unintended consequences of automating databases which have traditionally been regarded as "public" databases. The City of Victoria was caught off guard by public criticism accusing them of running roughshod over the privacy of property owners in Victoria, when in fact, the information it provided over the Internet could be accessed through a number of other sources, including the BC Assessment Authority, BC OnLine and the Land Title Registry.

[103] David Flaherty, Office of the Information and Privacy Commissioner of British Columbia, Investigation P98-011, An investigation concerning the disclosure of personal information through public property registries March 31, 1998, at http://www.oipcbc.org/investigations/reports/invrpt11.html.

> Nonetheless, the Office of the Information and Privacy Commissioner received a number of complaints from citizens concerned about their privacy. In response to these concerns, the City of Victoria removed the names of the homeowners from the Internet site ….
>
> …. There is a widely-held assumption that information in such "public" registers need not be protected at all, or that only very limited protections are needed."

The BC Civil Liberties Association weighed in, stating that, "What the City of Victoria did was to put this information on the Internet, so that it could be accessed by name, quickly, for free and anonymously. From a privacy perspective, this is a whole new ball game. The previous constraints on finding people, or snooping into their private business, have been eliminated…. In neither of these ways [previous means of access] can a stalker or an anti-abortionist anonymously find out a woman's or a physician's address."[104]

Research

In completing this report, the following individuals were interviewed or contacted for specific information:

Office of the Information and Privacy Commissioner (the oversight authority):

- Mary Carlson, Executive Director, Office of the Information and Privacy Commissioner
- Catherine Tully, Manager, Investigations and Mediation

Corporate Information Management Branch (the central agency):

- Sharon Plater, Director, Information Management/Information Technology Privacy and Legislation, Chief Information Office, Ministry of Labour and Citizens' Services
- Jason Eamer-Gould, Manager, Legislation and Privacy Policy

The following provided information, but were not subjects of a full interview

- Jacquie Edwards, Director, Information Planning and Services, Ministry of Finance (head of a privacy office serving several ministries)
- Charmaine Lowe, Interjurisdictional Alliance Director, Network BC, Chief Information Office, Ministry of Labour and Citizens' Services
- Cathy Yaskow, Vancouver Coastal Health Authority
- Evon Soong, Director or Privacy, Provincial eHealth Privacy, Security and Legislation Office, Ministry of Health

[104] John Westwood, *On-line property assessment information*, Letter to the Editor, *Vancouver Sun*, 2 October 1996, on BCCLA website at: http://www.bccla.org/othercontent/96johnproperty.html.

Extracts from British Columbia Policy and Legislation Regarding Privacy Impact Assessments

Freedom of Information and Protection of Privacy Act – extract with emphasis added

General information respecting use of personal information

69 (1) In this section:

"information sharing agreement" means an agreement that sets conditions on one or more of the following:

(a) the exchange of personal information between a public body and a person, a group of persons or an organization;

(b) the disclosure of personal information by a public body to a person, a group of persons or an organization;

(c) the collection of personal information by a public body from a person, a group of persons or an organization;

"personal information bank" means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual;

"privacy impact assessment" means an assessment that is conducted to determine if a new enactment, system, project or program meets the requirements of Part 3 of this Act.

(2) The minister responsible for this Act must maintain and publish a personal information directory to provide information about records in the custody or under the control of ministries of the government of British Columbia and about the use of those records.

(3) The personal information directory must include a summary that meets the requirements of the minister responsible for this Act of the following information:

(a) the personal information banks that are in the custody or control of each ministry of the government of British Columbia;

(b) the information sharing agreements into which each ministry of the government of British Columbia has entered;

(c) the privacy impact assessments that each ministry of the government of British Columbia has conducted;

(d) any other information the minister responsible for this Act considers appropriate.

(4) The head of a ministry must correct as soon as possible any errors or omissions in the portion of the personal information directory that relates to the ministry, and provide the corrected information to the minister responsible for this Act.

(5) The head of a ministry must conduct a privacy impact assessment and prepare an information sharing agreement in accordance with the directions of the minister responsible for this Act.

(6) The head of a public body that is not a ministry must make available for inspection and copying by the public a directory that lists the public body's personal information banks and includes the following information with respect to each personal information bank:

(a) its title and location;

(b) a description of the kind of personal information and the categories of individuals whose personal information is included;

(c) the authority for collecting the personal information;

(d) the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed;

(e) the categories of persons who use the personal information or to whom it is disclosed;

(f) information required under subsection (7).

(7) **The minister responsible for this Act may require one or more public bodies, or classes of public bodies, that are not ministries of the government of British Columbia**

(a) to provide additional information for the purposes of subsection (6), and

(b) to comply with one or more of the subsections in this section as if the public body were a ministry of the government of British Columbia.

(8) Not later than 60 days after making an order under section 33.1 (3) (orders allowing disclosure outside Canada), the minister responsible for this Act must publish a summary of the order.

Core Policy and Procedures Manual, 12.3.3 Information Management, Part II: Personal Information Protection:

"Two standard tools that assist ministries in the management of personal information are Privacy Impact Assessments (PIA) and Information Sharing Agreements. Ministries are required to conduct a PIA for new or revised projects, programs, applications, systems or new enactments. The PIA process determines if the privacy protection requirements of the Act are met. In all cases part 1 (basic information) of the PIA should be completed to assess whether personal information is being collected. Where it is determined that personal information is collected the complete PIA is required, whereas if it not being collected then only part 1 is required. The PIA supports government business objectives by ensuring the collection, use, retention, disclosure and security of information is conducted consistent with the Act and government policies, procedures and protocols. Information Sharing Agreements establish relationships, responsibilities, security requirements, access rights, and authentication requirements between ministries and the data consumers to whom they supply government information. Information Sharing Agreements may also be used in conjunction with alternate service delivery data management contracts and privacy protection schedules or with research agreements to clarify responsibilities of all of the involved parties."

Office of the Comptroller General, at http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1233ii

Description of PIA from Information and Privacy Commissioner's website

A PIA process is critical to enable a public body to properly assess, before any decision to proceed is made, whether a proposed program, policy or legislation has any privacy impact or complies with the *Freedom of Information and Protection of Privacy Act* (FIPPA).

A public body should perform a PIA, in consultation with its privacy experts, at the earliest possible stage for each proposed program, policy or piece of legislation. The PIA should be performed early in order to guide the decision on whether to proceed at all in light of any adverse privacy impact or concerns about compliance with FIPPA. The completed PIA should, in cases where the public body decides any privacy impact can be mitigated if it proceeds, be used to design the program, policy or legislation in a way that mitigates any privacy impact as far as possible.

The following link takes you to a PIA tool published by the IM/IT Privacy and Legislation Branch of the Ministry of Labour and Citizens' Services. (The OIPC commented on the PIA tool).

- Privacy Impact Assessment Template [link to http://www.mser.gov.bc.ca/privacyaccess/PIA/PiaTemplateRevisedMay06.doc]

Office of the Information and Privacy Commissioner of British Columbia, Resources for Public Bodies, at: http://www.oipc.bc.ca/sector_public/resources/pia.htm

Extract from central government information policy

Overview

A framework of legislation, policy and procedures governs information management within the government of British Columbia. The *Document Disposal Act* provides the legislative foundation for the management of government information. The Office of the Comptroller General (OCG) *Core Policy and Procedures Manual Chapter 12*, the Chief Information Office (CIO) IM/IT Management Policies, and policies and procedures developed by Corporate Information Management Branch, provide direction and standards to government ministries and agencies.

Legislation

The *Document Disposal Act* (RSBC 1996, c. 99) specifies the approvals required before government records may be disposed of (either destroyed, transferred to the government archives, or alienated from the Crown provincial).

Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165)

In addition, legislation that relates to specific records series is cited in individual *Operational Records Classification Systems* (*ORCS*).

General IM/IT Management Policies

The Office of the Comptroller General *Core Policy and Procedures Manual*(*CPPM*) contains government-wide policies for managing information, communications, materiel, transportation, contracts and expenses. Chapter 12 of *CPPM* specifically outlines the policies, authorities, responsibilities, and guidelines for managing information and information technology within the BC government.

The Chief Information Office (CIO) IM/IT Management Manual (PDF 437KB) contains additional standards/ guidance, roles and responsibilities for managing information management and information technology. The CIO IM/IT Management Manual is to be referred to in conjunction with the government's *Core Policy and Procedures Manual Chapter 12*.

From CIMB website, http://www.lcs.gov.bc.ca/CIMB/policy/default.htm

Central Government Policy regarding PIAs

Information and Technology Management Manual
Supplement to Chapter 12, Core Policy and Procedures Manual

12.3.2 II f. Privacy Impact Assessments (PIAs) [*Note: entire policy is reprinted here*]

General

Under section 69 of *Freedom of Information and Protection of Privacy Act*, ministries are required to conduct a Privacy Impact Assessment (PIA) to determine if a new enactment, system, project or program meets the Privacy Protection requirements in the *Freedom of Information and Protection of Privacy Act*. The PIA is designed to be used for all programs, legislation, systems or initiatives.

In order to provide a wide range of public services, government collects and maintains the personal information of British Columbians. Government must manage this personal information in accordance with the legislative requirements of *Freedom of Information* *and Protection of Privacy Act*. If a public body is developing a new enactment, system, project or program that involves personal information, the privacy protection provisions of *Freedom of Information and Protection of Privacy Act* apply. The PIA is designed to be used for all programs, legislation, systems or initiatives. It should be noted that only the Basic Information section will need to be answered (i.e., the PIA will be completed and the ministry's responsibilities will be met and documented) if no personal information is involved in the program, legislation, system or initiative.

Definition

Personal information - as defined in the Definitions section of the *Freedom of Information and Protection of Privacy Act* means recorded information about an identifiable individual;

Objective

To ensure that personal information collected, used and disclosed by government is protected in order to:

- comply with the requirements of *Freedom of Information and Protection of Privacy Act*;
- support government business objectives, including electronic government initiatives;
- identify and satisfy privacy requirements in a timely and cost efficient manner; and
- promote privacy awareness by using the PIA process as an educational tool.

Scope

This policy applies to all information that is collected and managed by government.

Authority, Responsibilities and Accountability

Ministries are responsible for ensuring that Directors/Managers of Information and Privacy and program managers are aware of and use PIAs when developing a program, legislation, system, or other initiative involving the collection, use and disclosure of information.

Ministry Directors/Managers of Information and Privacy are responsible for ensuring that the collection, use and disclosure of the personal information in ministry custody or under ministry control, including personal information that is in the custody of arms length service providers or contractors, is in accordance with *Freedom of Information and Protection of Privacy Act*.

Ministry Program Managers are responsible for ensuring that a Privacy Impact Assessment is completed during the early development stages of a program, legislation, system or other initiative as a component of the project or business plan.

The Information Policy and Privacy Branch (IPPB) is responsible for providing advice and assistance to ministries undertaking PIAs, where needed, and for a final review where personal information is collected, used or disclosed. Where required, IPPB may also conduct PIAs on corporate or cross-government initiatives. A corporate system is defined as a system that more than one ministry directly accesses for the purposes of inputting or correcting data/information.

Guidelines

Privacy Impact Assessment Form and Process

From: http://www.cio.gov.bc.ca/prgs/CPM12.pdf

V. PRIVATE SECTOR CASE STUDY: Royal Bank of Canada

Background

The Royal Bank of Canada (RBC) has over 1,400 branches across Canada, over 70,000 full-and part-time employees worldwide, and offices in over 34 countries. In revenue terms, its business units, collectively known as RBC Financial Group, form Canada's largest company.[105]

RBC has a long history of privacy initiatives, having had a formal privacy code since 1987. It was the first Canadian bank to employ an in-house privacy officer,[106] and was a participant in the drafting of the CSA *Model Code for the Protection of Personal Information*, which sets out ten principles that balance the privacy rights of individuals and the information requirements of private organizations. Key elements of the Code are now incorporated into the Canadian federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). RBC sees privacy as establishing important competitive differentiation in the sectors in which it operates, and thus aims to ensure that its business units have a culture and management disciplines that see privacy as an important part of daily operations.[107]

RBC's use of PIAs

RBC's adoption of PIAs was self-imposed and was seen as a natural evolutionary development of its privacy policy. The adoption of PIAs aimed to address an identified need at RBC for more privacy awareness, particularly with regard to the use of client information. RBC was an early adopter of PIAs in the Canadian private sector, developing its process in 2000 and rolling it out in 2001. It did not draw upon any particular existing PIA model when creating its PIA process. However, RBC did, and does, regularly liaise with Canadian privacy regulators.

Use of the PIA process is considered whenever there are new initiatives and projects, including outsourcing, as well as where there are significant changes or amendments to existing business processes, that may affect client or employee privacy. The PIA process is embedded in RBC's project management framework for business system development and IT system component review. It is separate from the privacy compliance and audit processes at the unit (branch) level.

Consideration of the need for a PIA is thus a requirement of RBC systems development. The process of determining whether a PIA is required involves project managers consulting with one of six Directors of Privacy who have responsibility for various RBC units. This will happen where there is use of client or employee information, and will involve an assessment of the scope of use and its potential impacts. The RBC Privacy team have significant involvement from the start and all aspects of a project will be reviewed. The decision to undertake a PIA is taken by the Director and not by the project manager and is fully documented. The speed and depth of initial review will depend upon the observed level of risk in conjunction with any other specific industry issues. If a project is particularly privacy sensitive, the matter can be referred to a senior committee at Senior V-P level which may set out specific requirements be met by the project.

[105] Mavin, D. (2007). The FP500 has a new ruler, *Financial Post Business Magazine* (June 05, 2007).

[106] Kuzz, E. R. & Colapinto, R. (2003). Privacy rules. *CA Magazine* 136(9):28-35.

[107] Hamilton, T.J. & Cavoukian, A. (2002) *The Privacy Payoff: How Successful Businesses Build Customer Trust*, McGraw-Hill Ryerson.

The PIA process is designed to assess the extent to which new uses of client/employee information generate particular privacy risks for RBC, for example, use of RFIDs in client services, or the transmission of data to the US would require a particularly detailed level of assessment. This produces a formal tiered assessment indicating low through high risk. The aim is then to develop appropriate and proportionate mitigating controls and strategies for those risks that are identified. Unlike the public sector, the PIA is not used to determine whether or not a project will be funded or not, to date use of PIAs at RBC has not prevented a business strategy being accomplished, however they have resulted in certain restrictions being placed on the use of client data.

There are various levels of support for PIAs within RBC, including:

- an internal privacy website which includes PIA advice;
- a PIA form incorporating a risk methodology which will indicate the level of internal approval/sign-off required on a project;
- the ability of staff, particularly less experienced staff, to draw upon RBC's internal privacy, security and audit teams.

There was a conscious decision to formalise the process of PIAs, but also to keep the length of the form short, aiming for a concentration on describing and evaluating potential privacy impacts rather than simply checking boxes. Particular care was taken in the construction of the questions, including the avoidance of repetition. The PIA form currently used is not automated.

Continuous 'evergreening' of the PIA process and paperwork during a system's use is not considered practical, but where there are significant changes, existing PIA documents would be returned to as part of the review process. Also, retention of the PIA form permits its use for compliance and audit purposes. The PIA form has space for feedback allowing those carrying out PIAs to comment on the process: to date such feedback has been relatively limited.

A key advantage of PIAs for RBC is that the process raises staff awareness of likely privacy issues arising from projects. This means that when they approach the privacy team, they tend to have already begun to think about those issues and possible solutions. This reduces the likelihood of unexpected privacy consequences and furthers RBC's corporate goal of developing and strengthening client trust. It is in this area rather than in the area of compliance with the requirements of national/international regulators, such as Canada's Office of the Superintendent of Financial Institutions (OSFI) and the US Securities and Exchange Commission (SEC), in which the main benefits of PIAs are obtained.

Research

In completing this report, the following individuals were interviewed or contacted for specific information:

Royal Bank of Canada

- Jeff C. Green, Vice President, Global Technology & Operations and Global Functions Compliance, and Chief Privacy Officer, RBC Financial Group
- Della Shea, Director, Privacy and Information Risk in IT, RBC Financial Group
- Tim Gough, Regional Head, Global Privacy & Information Risk Management - Europe & Asia, RBC Capital Markets.