APPENDIX A

Framework for Analysis

ORIGINS

1) When were PIAs first developed in the jurisdiction, by whom and for what purposes?

2) What is the status of PIAs in the jurisdiction? Are they required by law (if so which)? Are they policy? Are they guidance?

RULES FOR CONDUCT OF PIAs

3) Is there a clear definition of what a PIA is, and how it may differ from other compliance tools such as legal compliance checks and auditing?

4) What are the rules/expectations about who should conduct the PIA?

5) What factors are seen as determining which projects need PIAs?

6) What are the expectations/rules about consultation on PIAs throughout the process, and who are seen as stakeholders in the process? For example, corporations and agencies involved in the project, regulators, categories of affected individuals, civil society/NGOs representing or advocating for categories of affected individuals, the media, the general public.

7) What circulation, publication or submission rules or norms exist?

8) Is there an approval process for the PIA Report? If so, it is external or internal to the agency?

EFFECTS

9) Has there been any review of PIA experience?

10) As a regulator, what are the lessons learned to date? If you didn't have the existing tool in your jurisdiction and you were developing one now, what would it look like?

11) What do practitioners see as the key costs and benefits of PIAs for their organisations?

12) What sources have been influential:

- any guidelines from other jurisdictions?
- any academic, professional or government literature?

13) Can you provide or point to any:

- case studies of PIA processes?
- examples of PIA Reports?
- key contacts in organisations that have completed PIAS?

APPENDIX B

List of Interviewees, by Jurisdiction, Agency and Organisation Type

Name of Interviewee	Title	Organisation	Type
CANADA			
Andrée Morissette	Senior Privacy Policy Officer	Information, Privacy and Security Policy Division, Chief Information Officer Branch, Treasury Board of Canada, Secretariat	Central Agency
Navrose Austin	Senior Analyst		Central Agency
Trevor R. Shaw	A/Director General, Audit and Review	Office of the Privacy Commissioner of Canada	Oversight Body
Lindsay Scotton	Audit and Review	Office of the Privacy Commissioner of Canada	Oversight Body
Tracey Lee Grant	Senior Policy Advisor	ATIP Corporate Secretariat, Human Resources and Social Development Canada	Practitioner
Denis Lapalme	Senior Policy Advisor		Practitioner
Guy Herriges	Manager, Strategy and Policy	Office of the Chief Information and Privacy Officer, Ministry of Government Services, Ontario	Central Agency
Ken Anderson	Assistant Privacy Commissioner	Office of the Information and Privacy Commissioner of Ontario	Oversight Body
Mary Carlson	Executive Director	Office of the Information and Privacy Commissioner of British Columbia	Oversight Body
Catherine Tully	Manager, Investigations and Mediation	Office of the Information and Privacy Commissioner of British Columbia	Oversight Body
Sharon Plater	Director, IM/IT Privacy & Legislation	Office of the Chief Information Officer, Ministry of Labour and Citizens' Services, Government of British Columbia	Central Agency
Jason Eamer-Gould	Manager, Legislation and Privacy Policy		Central Agency
Tom Thackeray	Assistant Deputy Minister, Information Services	Information Services, Service Alberta	Central Agency
Hillary Lynas	Director, Access, Privacy and Security	Service Alberta	Central Agency
Franklin J. Work	Information and Privacy Commissioner of Alberta	Office of the Information and Privacy Commissioner, Alberta	Oversight Body

APPENDIX B

List of Interviewees, by Jurisdiction, Agency and Organisation Type

Leroy Brower	Health Information Act Director	Office of the Information and Privacy Commissioner, Alberta, BC	Oversight Body
George Alvarez	Director, Information and Privacy Office	Alberta Employment, Immigration and Industry	Practitioner
UNITED STATES OF AMERICA			
Rebecca Richards	Director of Privacy Compliance	Department of Homeland Security	Practitioner
Ari Schwartz	Deputy Director	Center for Democracy and Technology	Privacy Advocate
AUSTRALIA			
Andrew Solomon	Policy Director	Office of the Australian Privacy Commissioner	Oversight Body
Helen Versey	Privacy Commissioner of Victoria	Office of the Victorian Privacy Commissioner	Oversight Body
Phillipa O'Dowd	Privacy Services Manager	Office of the N.S.W. Privacy Commissioner	Oversight Body
Paul Bini	Senior Policy Advisor	Office of the Attorney-General of Queensland	Central Agency
J. Pritchard	Liaison Officer	Office of the Attorney General of Western Australia	Central Agency
Tamara Wenham	Executive Officer	Privacy Committee of South Australia	Oversight Body
Simon Allston	Tasmanian Ombudsman	Office of the Tasmanian Ombudsman	Oversight Body
Rachel Taylor	Policy Officer	Attorney-General's Department of the A.C.T.	Central Agency
Zoe Marcham	Information Commissioner of the Northern Territory	Office of the Information Commissioner of the Northern Territory	Oversight Body
NEW ZEALAND			
Blair Stewart	Assistant Commissioner (Policy)	Office of the Privacy Commissioner of New Zealand	Oversight Body
HONG KONG			
Allen Ting	Acting Chief Privacy Compliance Officer	Office of the Hong Kong Privacy Commissioner for Personal Data	Oversight Body

APPENDIX B

List of Interviewees, by Jurisdiction, Agency and Organisation Type

EUROPE			
Alexander Dix	Commissioner	Berlin Office for Data Protection and Freedom of Information, Berliner Beauftragter für Datenschutz und Informationsfreiheit	Oversight Body
Dr. Lynsey Dubbeld		Dutch Data Protection Authority, College Bescherming Persoonsgegevens (CBP)	Oversight Body
Ciara M. O'Sullivan		Irish Data Protection Commissioner's Office	Oversight Body
Marie Georges	Counsellor of the President for advanced studies, development and cooperation	French Data Protection Authority, La Commission Nationale de l'Informatique et des Libertés (CNIL)	Oversight Body
Astrid Flesland	Senior Legal Advisor	The Norwegian Data Inspectorate, Datatilsynet	Oversight Body
Reijo Aarnio	Data Protection Ombudsman	Finnish Office of Data Protection Ombudsman, Tietosuojavaltuutetun toimisto	Oversight Body

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 Municipal Freedom of Information and Protection of Privacy Act	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm 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 Local Authority Freedom of Information and 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 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.

Completion of PIAs

By Whom?

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]

When?

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.

Additional materials

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. *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_90f31_e.htm 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. *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/source/regs/english/2007/elaws_src_regs_r07322_e.htm 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.

<u>The Tool</u>

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.*

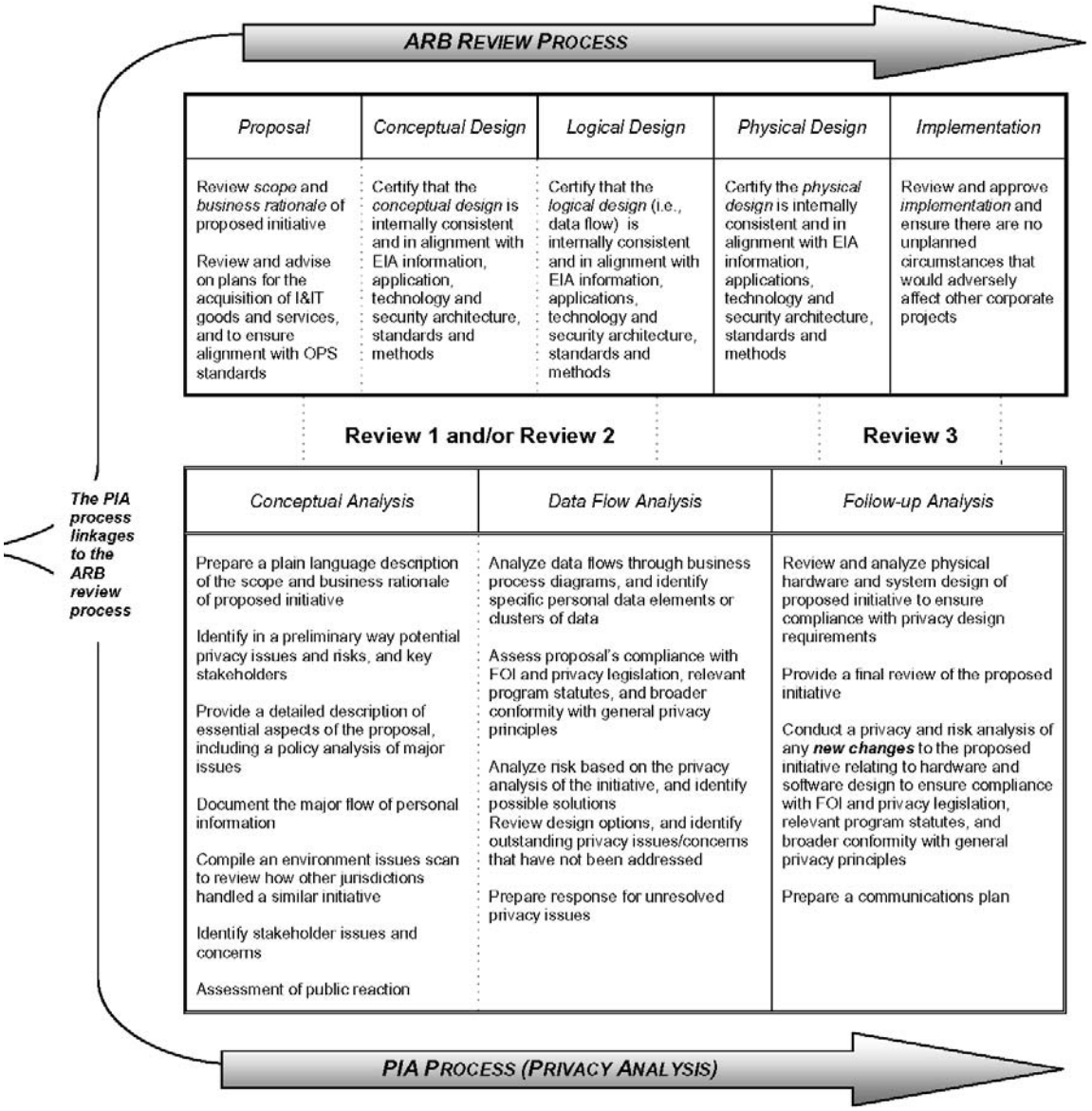
However, there is not a great deal of evidence that such formal review processes are commonplace.

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



[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:

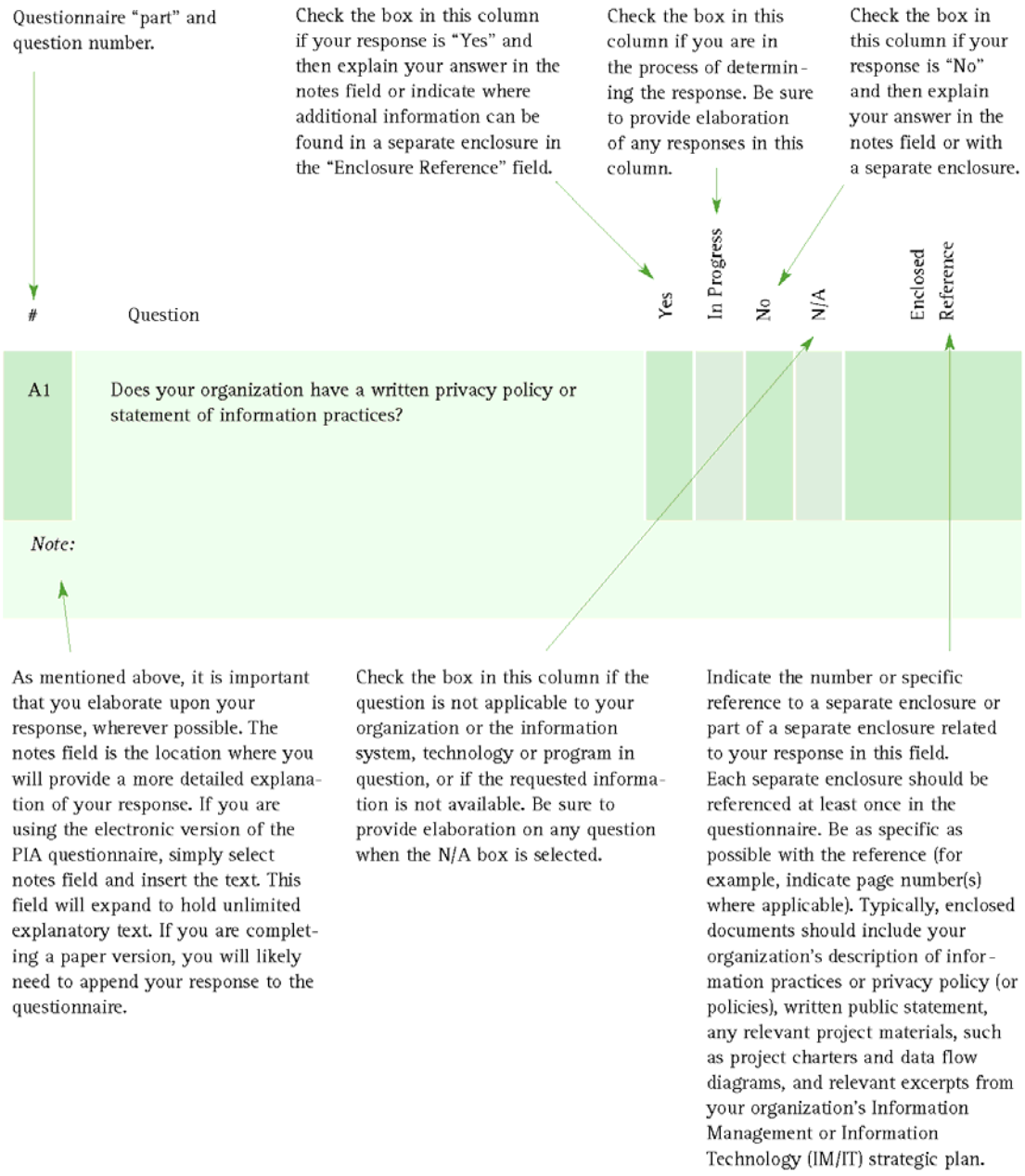
- Outlining data protection risks, which health information custodians are required to mitigate under *PHIPA*.
- Promoting the systematic analysis of privacy issues in order to inform debate on proposed or existing information systems, technologies or programmes;
- Helping relevant decision-makers understand 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]



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.

APPENDIX D

Privacy Impact Assessments: Jurisdictional Report for the United States of America

CONTENTS

The Legislative and Policy Framework

A complex body of law (constitutional, tort and statutory) governs the collection, processing and disclosure of personally identifiable information in the United States. The main federal laws governing privacy protection within the federal public sector are:

- The *Privacy Act* of 1974, 5 U.S.C. § 552a applies fair information principles to the personal information held by federal government agencies.
- *The Computer Matching and Privacy Protection Act,* 5 U.S.C. 552a(o) describes the manner in which computer matching involving Federal agencies should be performed
- The *Driver's Privacy Protection Act*, 18 U.S.C. 2721-2725 prohibits the release and use of certain information from state motor vehicle records.
- The *Computer Security Act*, Public Law 100-235 establishes a minimum acceptable security practices for federal information systems and requires the creation of computer security plans, and the appropriate training of system users where the systems house sensitive information.
- The *Electronic Communications Privacy Act* , 18 U.S.C. § 2510, sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications.
- *The Electronic Government Act* of 2002, 44 U.S. § 101, establishes new agency requirements, including PIAs, for the development of e-government initiatives.

There is no comprehensive privacy protection law governing the private sector. However, the main federal provisions are:

- The *Federal Trade Commission Act*, 15 U.S.C. § 41, et seq., empowers the FTC to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.
- Title V of the *Gramm-Leach Blighly Act*, 15 U.S.C. § 6801, et seq., enacted in 1999, contains privacy provisions relating to consumers' personal financial information.
- The *Children's Online Privacy Protection Act* 15 U.S.C. § 6501, et seq., was enacted in 1998 to protect the personal information of children under the age of 13 that is collected online.

  The *Identity Theft Act*, 18 U.S.C. § 1028, 1028(a)(7) made it a federal crime to knowingly transfer or use, "without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."
- The *Cable Communications Policy Act* of 1984 47 U.S.C. § 551, restricts the collection, maintenance, and dissemination of subscriber information.
- The *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) 42 U.S.C. § 1320d, et seq., and regulations issued by the Department of Health and Human Services (HHS) create standards to protect the privacy of individuals' personal health information.
- The *Fair Credit Reporting Act* (FCRA) 15 U.S.C. § 1681, et seq., first enacted in 1970 and most recently amended in 1996, is designed to promote the accuracy and ensure the privacy of the sensitive financial information contained in consumer credit reports.

- The *Federal Videotape Privacy Protection Act*, 18 U.S.C. § 2710, enacted in 1988, addresses information about consumers' videotape purchases and rentals.

Tort law also plays a more important role in the United States than in other countries, as does the 200 year old history of interpretation of the "unreasonable search and seizure" clause within the 4th Amendment of the federal Constitution. There are also an enormous number and range of statutes at the various state levels. Three legislative provisions are especially relevant for the conduct of PIAs within the federal government.

The first and most general is the *Administrative Procedure Act* of 1946, which governs the general method by which federal agencies may propose and establish regulations. The basic purposes of the APA are:

(1) to require agencies to keep the public informed of their organisation, procedures and rules;
(2) to provide for public participation in the rulemaking process;
(3) to establish uniform standards for the conduct of formal rulemaking and adjudication;
(4) to define the scope of judicial review.

Most federal agencies have developed rules through "informal rulemaking" including: Publication of a "Notice of Proposed Rulemaking" in the Federal Register; opportunity for public participation by submission of written comments; consideration by the agency of the public comments and other relevant material; and publication of a final rule not less than 30 days before its effective date, with a statement explaining the purpose of the rule.

Secondly, the *Privacy Act* of 1974 establishes the basic statutory "fair information principles" for federal agencies and obliges the publication of a Systems of Record Notice (SORN) when most new personal information systems are established. All Federal agencies are required to publish in the Federal Register each system of records when the system is established or changed. These notices include the following: Name and location of the system; Categories of individuals on whom records are maintained in the system; Categories of records maintained in the system; Each routine use of the records contained in the system, including categories of users and purpose of such use; Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; Title and business address of the agency official responsible for the system of records; Agency procedures whereby an individual can be notified at his or her request if the system of records contains a record pertaining to him or her; Agency procedures whereby an individual can be notified at his or her request how he or she can gain access to any record pertaining to him or her contained in the system of records, and how he or she can contest its contents; and Categories of sources of records in the system. There are exemptions for systems established for national security reasons.[1]

Thirdly, the *Electronic Government Act* of 2002 states that each federal agency shall undertake a PIA "before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information." Agencies are to ensure review by the Chief Information

[1] *The Privacy Act* of 1974 (5 U.S.C. § 552a). See also: Office of Management and Budget, Instructions for complying with the President's Memorandum of May 14, 1998 "Privacy and Personal Information in Federal Records" at: http://www.whitehouse.gov/omb/memoranda/m99-05-b.html.

Officer, or equivalent official, as determined by the head of the agency; and "if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." This requirement may be waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment."[2] This legislation was designed to supplement the broader requirements within the *Privacy Act*.

Responsibility for providing guidance on the interpretation of privacy protection policy in the federal government rests with the Office of Information and Regulatory Affairs (OIRA) within the Office of Management and Budget (OMB), the agency within the Executive Office of the President responsible for developing the President's budget proposals and for the central coordination and oversight of a range of procurement, financial management, information and regulatory policies. It is seen as "central agency" for the purposes of this study.

The analysis begins with the history and context of PIAs in the United States, and describes the general process established under the *Electronic Government Act* of 2002 for the conduct of PIAs in the federal government as a whole. It then discusses the approaches of three agencies (the Internal Revenue Service {IRS}, the Department of Homeland Security {DHS} and the US Postal Service {USPS}), whose experiences have been distinctive. The case study concludes with some general lessons about the conduct of PIAs in the United States, and their applicability to the UK.

History and context of PIAs in the United States

It is impossible to gauge the extent of the use of PIAs within the American private sector, although it is probable that assessments of privacy implications have been an integral part of new product and service review for many companies for a long time. They tend to be internal, and often proprietary, analyses whose final products are rarely made public. PIAs must also be considered in the light of a whole range of self-regulatory mechanisms, including codes of practice, certification tools, privacy notices and privacy seals, which have spread throughout the US commercial sector in recent years.[3] Just because there are few instruments called PIAs published within the US corporate sector, does not mean that equivalent risk assessments are not performed.

Whereas there is an unknown number of PIAs in the US private sector, it can be asserted that there are very few examples at the state level, although California's Office of Privacy Protection, one of the only oversight bodies[4] with responsibility for privacy protection, is beginning to see PIA methodology as a part of their best practices recommendations for state authorities. For the first time, the use of PIAs is defined as a task within California's plan for information technology. By autumn 2007, the State Privacy Officer, in consultation with the State Information Security Office is supposed to develop a methodology and a set of tools that departments can use to "self assess the

[2] The Electronic Government Act of 2002, 44 USC 101.
[3] Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006), ch. 6.
[4] Although this organisation fulfils some "oversight" functions, such as taking complaints, it also has a "central agency" role and is not independent of the administrative arm of the California State government.

privacy impact of proposed new and major modifications to existing IT systems that contain personal information."[5]

Thus the development of PIAs in the United States is principally confined to the activities of the federal government. Their history dates to the mid-1990s when the IRS began to require them for certain large projects, and issued a set of PIA guidelines in 1996 (later revised). The main impetus, however, was provided by the enactment of the *Electronic Government Act* of 2002. The central purpose of this law is to improve the management and promotion of electronic government services through the Internet. According to the presidential signing statement: "This legislation builds upon my Administration's expanding e-government initiatives by ensuring strong leadership of the information technology activities of Federal agencies, a comprehensive framework for information security standards and programmes, and uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. The Act will also assist in expanding the use of the Internet and computer resources in order to deliver Government services, consistent with the reform principles I outlined on July 10, 2002, for a citizen-centered, results-oriented, and market-based Government."[6]

The PIA provisions did not generate a lot of attention at the time, even though it was obvious that they would have implications beyond the "e-government" context. They were seen by the privacy advocacy community as a way to push for some incremental improvements to federal privacy protection policy, given their calculation that oversight by a more general privacy protection agency was not considered feasible, nor enactable.[7] Within a complex landscape of privacy protection laws which tend to fix privacy problems in a pragmatic and reactive manner after they have occurred,[8] these PIA provisions do stand out as comparatively forward-looking. Their execution is, however, variable and very much dependent on factors peculiar to individual agencies.

We will review the general process for conducting PIAs within federal agencies, as a whole, and then focus more specifically on three agencies which have developed more distinctive PIA methodologies (the IRS, the DHS and the US Postal Service).

The American PIA Process

PIAs must analyse and describe: what information is to be collected including the nature and the source; why the information is being collected; the intended use(s) of the information; with whom the information will be shared, such as another agency for a specified programmatic purpose; what opportunities individuals have to decline to provide information or to consent to particular uses of the information (other than required or authorised uses), and how individuals can grant consent; how the information will be secured through administrative and technological controls; and whether a system of records is being created under the *Privacy Act*.

<u>The Tools</u>

[5] http://www.cio.ca.gov/pubs/StrategicPlan.html
[6] President signs E-Government Act, http://www.whitehouse.gov/news/releases/2002/12/20021217-5.html.
[7] Interview with Ari Schwartz, Center for Democracy and Technology (CDT), August 10, 2007.
[8] See, for example, the arguments about the American policy style in Colin J. Bennett, *Regulating privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).

Under the *Electronic Government Act*, a privacy impact assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the information will be shared, what notice would be provided to individuals and how the information will be secured. Seven months after the statute's operative date, the Office of Management and Budget (OMB) issued guidelines on how PIAs should be conducted.[9] The general presumption is that responsibility for PIA compliance is delegated to individual agencies. Separate guidelines (from those of the OMB) have been prepared by the Privacy Office of the DHS[10], by the Privacy and Civil Liberties Office within the Department of Justice,[11] by the US Postal Service[12] and by the IRS[13] among others.

Completion of PIAs

Who Participates in the PIA?

It is generally presumed that PIAs in the federal government will be conducted by relevant programme managers in consultation with experts in the areas of information technology, IT security, records management and privacy. Although the OMB guidance allows considerable discretion, it is clear that the *Electronic Government Act's* privacy provisions were intended to make systems development a multidisciplinary effort.[14]

When and under what circumstances are PIAs conducted?

The Electronic Government Act requires agencies to conduct a PIA before: "developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government)." The OMB guidance provides some examples of the kinds of system changes that might create new privacy risks:

- when converting paper-based records to electronic systems;
- when functions applied to an existing information collection change anonymous information into information in identifiable form;
- when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralised, matched with other databases or otherwise significantly manipulated;

[9] OMB**,** Electronic Government Act Section 208 Implementation Guidance, http://www.whitehouse.gov/omb/memoranda/m03-22.html. This delay has been interpreted as signalling a lack of commitment to the statute. Kenneth A Bamberger and Deidre Mulligan, "Privacy Decision-Making in Administrative Agencies," Chicago Law Journal forthcoming.
[10] At: http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.
[11] At: http://www.usdoj.gov/pclo/pia.htm.
[12] At: http://www.usps.com/privacyoffice/pia.htm.
[13] At: http://www.irs.gov/irm/part11/ch02s01.html.
[14] As quoted by OMB staff in Jason Miller, "Serious about Privacy," *Government Computer News*, May 17, 2004 at: http://www.gcn.com/print/23_11/25917-1.html.

- when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources;
- when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting e-government initiatives; development of this cross agency IT investment;
- when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

The guidance also specifies the conditions under which PIAs may *not* be required: "when IT systems do not collect or maintain information in identifiable form about members of the general public; where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g. questions or comments) or obtaining additional information; for certain national security systems; when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the *Privacy Act*; when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes; when agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form; and for minor changes to a system or collection that do not create new privacy risks. Agencies must also update their PIAs to reflect "changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form."

Agencies should commence a PIA when they begin to develop a new or significantly modified IT system, and its depth and content should be "appropriate for the nature of the information to be collected and the size and complexity of the IT system." A distinction is also made between: 1) "major information systems" the PIAs for which should reflect more extensive analyses of: the consequences of collection and flow of information, the alternatives to collection and handling as designed, the appropriate measures to mitigate risks identified for each alternative and, the rationale for the final design choice or business process; 2) "routine database systems" where a more standardised approach such as a checklist or template is appropriate. In both cases agencies must consider the information "life cycle" and evaluate how information handling practices at each stage may affect individuals' privacy.

Review and Approval of PIAs

The E-Government legislation and the OMB Guidance specifies that agencies must also ensure that the PIA document be approved by a "reviewing official" (the agency Chief Information Officer or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA). Agencies are given wide latitude under the Act to assign responsibilities for the conduct of PIAs.

OMB is the major central budget coordination agency within the federal government. Thus, incentives for the preparation of PIAs are built into the annual budget approval

cycle and agencies must have privacy compliance documentation in place before going to OMB for funding. It is, however, difficult to ascertain whether budgets are indeed sent back for review because the PIA was insufficient or incomplete because these internal budget decisions are rarely made public. PIAs might also be triggered by the requirement within the *Federal Information Security Management Act* (FISMA) that agencies must report annually to the OMB and to Congress on the effectiveness of the agency's security programmes. From time to time, there have also been oversight by the Governmental Accountability Office[15] and by certain Congressional committees.[16]

External Consultation

There is no provision in either the Electronic Government Act, or the accompanying OMB Guidance for any external stakeholder consultation on draft PIAs. Rarely, therefore, are those outside the agency asked to comment or provide any input before a PIA is published.

The only notable exception where external consultation occurred in advance of PIA publication was as a result of HSPD-12, the Presidential directive mandating a common identification standard for federal employees and contractors.[17] This directive mandated the National Institute of Standards and Technology (NIST) to promulgate a Federal standard for secure and reliable forms of identification. The widespread implications of this standard prompted a full-day meeting, hosted by OMB, with privacy and civil liberties advocates before the PIA process was concluded. The meeting was reportedly a valuable, but rare, occasion when outside input was sought.[18]

Public Availability and Accountability

In contrast to PIAs in other countries, there is a requirement that the resulting documentation should be made public, although agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement efforts or competitive business interests). Such information is meant to be handled in a manner consistent with the *Freedom of Information Act* (FOIA).

Many agencies now post PIAs on their respective websites. Hence, and after just five years in operation, there are now a large number of PIAs, of varying length and substance, which are published and available for review. These published PIAs are for the: Department of Homeland Security[19]; Internal Revenue Service[20]; US Postal Service[21]; Department of Transportation[22]; Department of Labor[23]; Department of

[15] US Governmental Accountability Office, *Homeland Security: DHS Privacy Office has Made Progress but faces Continuing Challenges*, Statement by Linda Koontz, Director Information Management Issues, GAO-07 1024T at: http://www.gao.gov/new.items/d071024t.pdf.
[16] Particularly by the Subcommittee on Commercial and Administrative Law of the House Judiciary Committee.
[17] At: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.
[18] Interview, Ari Schwartz, August 10th, 2007
[19] Department of Homeland Security at: http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#10.
[20] Internal Revenue Service at: http://www.irs.gov/privacy/article/0,,id=122989,00.html.
[21] US Postal Service at: http://www.usps.com/privacyoffice/pialist.htm.
[22] Department of Transportation at: http://www.dot.gov/pia.html.
[23] Department of Labor at: http://www.dol.gov/cio/programmes/pia/mainpia.htm

State[24]; Department of Justice[25]; Department of Health and Human Services[26]; Department of Education[27]; Bureau of the Census[28]; and several others.

These requirements for publicity should also be seen in conjunction with the *Privacy Act* requirement for federal agencies to publish a Systems of Records Notice (SORN) in the *Federal Register* for each agency system that collects more than one record that contains information about an individual and is designed to be retrieved by name or other personal identifier. The SORN is typically a briefer statement preceding a more thorough PIA.

Individual Agency Experiences

There is no easy conclusion about the impact of PIAs within the US federal government because the models vary. The experience of three agencies, the IRS, the DHS and the USPS represent subtly different approaches to PIA development and implementation.

The Internal Revenue Service (IRS)

The IRS was one of the first agencies anywhere in the world to develop PIAs, attributable to the fact that in 1993, as a result of some highly publicised abuses of taxpayer information, the agency decided to institutionalise an Office of the Privacy Advocate. The IRS has, therefore, had a lengthy experience with conducting PIAs both before and since the Electronic Government Act was passed. In 2000, its PIA process was endorsed as a best practice by the Federal Chief Information Officer's Council.[29]

Within the IRS, the PIA process is explicitly designed to guide business owners and system developers in evaluating privacy risks through the stages of system development. Owners of new systems, systems under development, or systems undergoing major modifications are required to complete a PIA, but there is no pre-screening tool as in DHS. The purpose of the PIA is to identify privacy risks in the system and to limit the information collected and used to only what is relevant to achieve a legitimate business purpose. The business Owner and system Developer must initiate the PIA in the early stages of the development of a system and complete it as part of the system's required Enterprise Life Cycle review.[30]

Review of PIAs within the agency is the responsibility of the Director of the Office of Privacy, formally called the Office of the Privacy Advocate. This office was established in 1993 and developed its own set of Privacy Principles, disseminated in May 1994. This office reserves the right to request that a PIA be completed on any existing system that they determine may have privacy risks. It is responsible for the development of policies to protect taxpayer and IRS employee privacy and ensures that they are integrated into all IRS practices and policies. It also answers questions on PIA procedures, provides training, and serves as an agency resource on privacy issues. Business owners and system developers submit the completed PIA to the Privacy Office for analysis, which

[24] Department of State at: http://foia.state.gov/piaOnline.asp.
[25] Department of Justice at: http://www.usdoj.gov/pclo/pia.htm.
[26] Department of Health and Human Services at: http://www.hhs.gov/foia/.
[27] Department of Education at: http://www.ed.gov/notices/pia/index.html.
[28] Bureau of the Census at: http://www.census.gov/po/pia/.
[29] Federal Chief Information Officer's Council, Internal Revenue Service Model Information Technology Privacy Impact Assessment, February 25, 2000 at: http://www.cio.gov/Documents/pia_for_it_irs_model.pdf.
[30] Part 11., "Communications and Liaison," IRS, at: http://www.irs.gov/irm/part11/ch02s01.html.

reviews the completed PIA to identify privacy risks and to ensure only relevant and necessary information is collected and used. There is then an attempt to reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached, the unresolved issues will be presented to the Chief Information Officer for his decision. The Business owner and system developer also are expected to conduct life cycle review of systems to ensure satisfactory resolution of identified privacy risks.[31]

It appears, therefore, that IRS places more stress on the *process*, than on the final privacy impact *statement*. According to the relevant guidance material: "Privacy issues must be addressed when systems are being developed or updated, and privacy protections must be integrated into the life cycle of these automated systems. The vehicle for addressing privacy issues in a system is the Privacy Impact Assessment (PIA). The PIA process also provides a means to monitor compliance with applicable laws and regulations governing taxpayer and employee privacy."[32]

The Department of Homeland Security (DHS)

The DHS Privacy Office is the first statutorily required Privacy Office at any federal agency. Its mission is to minimise the impact on the individual's privacy and oversee the operation of Section 222 of the Homeland Security Act, the *Privacy Act* of 1974, the Freedom of Information Act, the Electronic Government Act of 2002 and other Executive Orders, court decisions and DHS policies that protect the collection, use, and disclosure of personal information. It operates under the direction of the Chief Privacy Officer (CPO), who is appointed by the Secretary. With respect to the activities of the DHS, the Privacy Officer also has authority under Section 222 of the Homeland Security Act of 2002 to require PIAs. Because of this provision, PIAs tend to be defined and used more broadly in the DHS than in other federal agencies.[33]

The DHS has adopted a Privacy Threshold Analysis (PTA) instrument, a simple five-page form designed to determine whether a PIA will be required.[34] This analysis could lead to one of two outcomes: a determination that this is not a Privacy Sensitive System because it contains no personally identifiable information; or, it is a Privacy Sensitive System. If the latter, there might be a determination that the PTA is sufficient, or that it is a national security system or human resources system and therefore exempt from the Electronic Government Act, or that it is a legacy system and no changes have been made and thus a PIA is also not required. PTAs have been conducted on all 735 systems within the Department of Homeland Security.[35]

In the DHS, if the PTA indicates that a PIA is necessary, then they are performed normally by the programme manager in coordination with the Information security person. Drafts are prepared, circulated internally and normally reviewed by legal counsel. This is normally an iterative process that can last 4-6 weeks. The document triggers an internal conversation about privacy practices.[36] The draft is then reviewed by the Office of the Director of Privacy Compliance, which will typically provide comments. The vast majority of PIAs do go back to the programme manager for more information and clarification. If the various issues are not addressed, then face-to-face meetings are

[31] http://www.irs.gov/irm/part11/ch02s01.html.
[32] Ibid.
[33] Interview, Rebecca Richards, Director of Privacy Compliance, DHS, August 9, 2007.
[34] http://www.dhs.gov/xlibrary/assets/privacy/DHS_PTA_Template.pdf.
[35] Interview, Rebecca Richards, Director of Privacy Compliance DHS, August 9, 2007.
[36] Interview, Rebecca Richards, DHS, August 7, 2007.

arranged. At the end of the process, the CPO signs off on all PIAs, and will frequently request further changes at this stage. The programme is not allowed to go operational until the CPO has signed off. However, there are a large number of legacy systems which predated the creation of the DHS, which are far more difficult to evaluate. The vast majority of DHS PIAs are published on the DHS website.

The DHS Privacy Office does hold some public workshops at which PIA process may be discussed in the context of the larger debates about the relationship between privacy and homeland security. There is also a DHS Data Privacy and Integrity Advisory Committee which advises the Secretary and the CPO on programmatic, policy, operational, administrative, and technological issues within the Department that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues. This committee includes representatives from the private sector, academia and the non-governmental organisation sector.

The United States Postal Service (USPS)

The U.S. Postal Service has access to an enormous amount of highly sensitive information - home addresses, credit card numbers, stop-mail orders, change of address forms, the magazines people read and the catalogs from which they order. It is also one of the most trusted organisations in the United States. Significant attention to privacy issues within the USPSS was attributable again to the appointment of a Chief Privacy Officer in 2001, in this case Zoe Strickland who began to re-examine the organisation's Systems of Records and the data flows within the agency. Ms. Strickland helped put together for project managers a full "business impact assessment" process that examines a wide range of potential issues, including privacy and security impact assessments.

The USPS “voluntarily complies” with the Electronic Government Act of 2002. The Postal Service’s PIAs are known as Business Impact Assessments (BIA). They are required for all IT systems, both customer and employee. Separate guidance has been issued in the form of BIA template guidance in short and long forms, both of which go some way beyond the OMB guidance. They appear also to be a good deal broader than a legislative compliance checklist. To quote: “The BIA addresses all privacy and security requirements, including ensuring privacy compliance, determining the sensitivity and criticality of the system, and developing the appropriate security plan. The BIA has long been postal policy, and is required for all IT systems, including those containing customer or employee information.”[37]

According to Strickland, the process involves five steps:

1) Develop a questionnaire. Each questionnaire should solicit information about a system under development, addressing plans for privacy and security. It also should capture, assess and drive data practices;
2) Define the scope. The assessment should cover all systems within a particular programme, as well as all technologies being used to collect, create or manage information;
3) Establish the schedule. The agency should plan when work on the assessment should start and be completed;

[37] http://www.usps.com/privacyoffice/pia.htm.

4) Determine roles and accountability. Employees should know what is expected of them and who will sign off on the finished assessment;

5) Define how the process works. Each objective should be clearly identified and the PIA process, including approach to risk management, should be easily repeatable.[38]

Lessons Learned from the United States of America

The differences between American and UK data protection policy as well as larger variations in the institutional and administrative culture suggest that there might be few lessons, positive or negative, which usefully can be drawn from the American experience. Privacy laws have emerged pragmatically, reactively and according to the different needs of individual sectors. The overall picture, therefore, has been described as "fragmented, incomplete and discontinuous."[39] American PIA policy needs, therefore, to be evaluated according to US standards, rather than those of countries with comprehensive data protection laws overseen and administered by data protection or privacy agencies with dedicated responsibilities for these issues. Within those parameters, PIAs have stood out as one of the more positive aspects of American privacy protection policy within the last ten years.

Several conclusions about their implementation can be reached from this brief survey.

- The legislative mandate is peculiar in comparative context. It produces a significant number of PIAs, but obviously of variable quality. There is a tendency in some agencies to treat PIAs as things they have to do, rather than things they should do to mitigate risk.
- The presence and type of privacy infrastructure within an agency is probably the most important influence on the successful conduct of PIAs.
- The publication of PIAs contributes to transparency. But the lack of prior consultation with external stakeholders can harm their perceived legitimacy.
- The accountability established within the PIA and SORN frameworks tend to rely on outmoded conceptions of a "system of records" which may not be sufficiently sensitive to the fluid and interactive realities of contemporary data flow environments.

The Legislative Mandate

There is no other example of a national jurisdiction where PIAs are mandated by statute across an entire governmental and administrative system. This mandate produces a significant incentive to produce the relevant documentation as part of the annual budget review cycle. The mandate forces agencies to consider their compliance with the relevant privacy principles within the *Privacy Act*.

Statutory mandates, however, raise the question of whether agencies complete these reviews because they have to, or because it is in their more general interests to mitigate

[38] Jason Miller, "Serious about Privacy." *Government Computer News*, May 17, 2004 at: http://www.gcn.com/print/23_11/25917-1.html.

[39] Robert Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199 (1993). See also: Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

privacy risks. Former OMB administrator for e-government and IT, Karen Evans has remarked that PIAs should not just be a check box to OMB to say 'we've done it' but a methodology to think seriously about how they will use citizens' data and incorporate that thinking as they plan new systems and upgrades.[40] There is, however, the danger that statutory compulsion produces a "checklist" approach. The legislative mandate can produce a mentality that PIAs are merely statements, just one more piece of documentation that needs to be in place during the annual budget review process.

Furthermore, the demand for effective and comprehensive PIAs can only be achieved with sufficient staffing resources, and this creates delays. For example, a Governmental Accountability Office Report on the work of the DHS Privacy Office noted some significant progress in the incorporation of privacy management into the Department, as well as the increase in the number of PIAs that had been produced since its inception. It also stressed the challenges in producing PIAs and SORNs in a timely fashion, especially as they relate to the existing legacy systems within the Department.[41] One can only infer that similar or greater challenges are faced in Departments with fewer privacy staff.

The Presence and Type of Privacy Infrastructure

PIA rules have been applied "highly inconsistently across agencies, and even between programmes" according to Ken Bamberger and Deidre Mulligan.[42] Their case studies of PIAs within the Department of State and the DHS tend to support an overall conclusion that PIAs are more likely to be conducted more seriously, and thus have an impact on agency culture, if there is a "privacy infrastructure" – comprised of specialised personnel who not only know about the law and the technology, but can forcefully articulate the larger ethical and moral questions. There seems to be a common agreement that the privacy infrastructure within agencies such as the IRS, DHS and USPS has the potential to institutionalise meaningful PIA compliance. This experience supports the proposition that it is often better to have the privacy rationale articulated from within, than from without. It allows the agency experts to scrutinise PIAs before they go out of the door. But Bamberger and Mulligan also caution that such compliance is highly contingent on the leadership skills of a forceful CPO. In many respects, these conclusions echo well-established generalisations about the successful implementation of any privacy protection policy or law.[43] While the expertise of a privacy office is essential to the completion of PIAs, that office should be respected and seen as a legitimate "internal privacy advocate", by virtue of its history, organisational independence and reputation of senior personnel.

For those few officials within the federal bureaucracy who are steadfastly attempting to advance the privacy argument, PIAs do provide a valuable tool. As Ari Schwartz, Deputy Director of the Center for Democracy and Technology has commented, they do "motivate people who want to do the right thing, to do the right thing."[44] However, most

[40] Quoted in Jason Miller, "Serious about Privacy," ref 38.
[41] US Governmental Accountability Office, *Homeland Security: DHS Privacy Office has Made Progress but faces Continuing Challenges*, Statement by Linda Koontz, Director Information Management Issues, GAO-07 1024T at: http://www.gao.gov/new.items/d071024t.pdf
[42] Kenneth A Bamberger and Deidre Mulligan, "Privacy Decision-Making in Administrative Agencies," *Chicago Law Journal* (forthcoming).
[43] See David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989).
[44] Interview, Ari Schwartz, August 10, 2007

federal agencies do not have privacy offices with a statutory basis and with adequate staff. In 1998, the Clinton Administration required all agencies to designate a senior official within the agency to assume primary responsibility for privacy policy and to review *Privacy Act* compliance within each agency. In 1999, the Administration appointed a Chief Privacy Counselor for the Administration within the OMB. In 2001, despite urging from privacy advocates, the Bush Administration did not hire a new Chief Privacy Counselor in the OMB. American privacy advocates continue to press, therefore, for effective privacy officer functions in every federal agency with: (1) a statutory basis; (2) adequate staff; and (3) involvement in senior-level policy deliberations.[45] These conditions are generally regarded as necessary for the advancement of privacy protection policy generally, as well as for the conduct of PIAs in particular.

Transparency of output, but a lack of external consultation during the PIA process

The presumption of publicity embedded within the Electronic Government Act helps to render transparent some personal information systems that would otherwise be clouded in secrecy. For those outsiders with the time, energy and commitment, they do serve as one, albeit imperfect, instrument of accountability. The more thorough PIAs provide important raw material for privacy professionals within government, for Congress and for privacy advocates to ask the right questions about the collection, use and disclosure of personal information.

As there is no requirement under the E-Government legislation for outside consultation, however, then procedures have naturally developed to emphasise the importance of PIAs as "pre-decisional" instruments for the benefit of internal review and analysis. And while there seems to be a general consensus among American privacy advocates that it is, on balance, better to have PIAs conducted and published than not, there is also a series of question marks about whether the internal procedures really do result in significant changes to a programme in response to internal arguments about privacy risks.

There have been occasions when the delays of publication of PIAs have been criticised. In November 2006, the DHS provided additional notice in the *Federal Register* of the Automated Targeting System (ATS), the process of security ratings of American citizens of millions of travelers, based on the same risk-assessment methodologies designed for the screening of cargo coming into the United States. DHS announced that the programme would go into effect on December 4, 2006. In its comments, the American Civil Liberties Union complained that: "the program's Privacy Impact Assessment (PIA) was not made available to the public until November 27 – only one week before the program is slated to go into effect. Given that the PIA represents the most comprehensive explanation of the system provided to the public, that is simply not a reasonable amount of time. It does not allow respondents to adequately analyze the privacy impact statement and its implications, formulate comments articulating that analysis clearly, and submit them with time for Department of Homeland Security to properly consider them before the program becomes effective."[46] Similar criticisms were levied against the PIA process for the US Visit programme, a "forthright and clear analysis of the privacy issues involved" according to Jim Dempsey of CDT, but one that

[45] Statement by Jim Dempsey of Center for Democracy and Technology, House Committee on the Judiciary Subcommittee on Commercial and Administrative Law, February 10, 2004 at: http://www.cdt.org/testimony/20040210dempsey.shtml#f2#f2.
[46] http://www.aclu.org/privacy/gen/27593leg20061201.html.

would have been "far more meaningful if it had been issued before the program was actually being implemented."[47]

While public input post-PIA and post-programme design can result in privacy-enhancing changes, it also takes concerted effort on the part of external privacy advocates, and the programme costs can often be greater. Where programmes have undergone significant change, in some part as a result of external criticism, the PIAs do provide interesting comparative reference points. The programme called "Secure Flight" is a case in point. First announced in 2004 as a successor to the Computer Assisted Passenger Profiling System (CAPPS), Secure Flight was designed as a passenger pre-screening tool to authenticate information on air travelers with records stored in government databases, and with data purchased from unspecified commercial data aggregators. There was an enormous amount of criticism, not only from the privacy advocates, but also from a series of reports within the General Accounting Office (GAO). The programme was reconsidered and reintroduced in August 2007, together with a new PIA.[48] As with other controversial surveillance systems associated with the Bush Administration's "War on Terror,"[49] these programmes carry high political stakes and have been the product of an extraordinary amount of attention from media and civil liberties groups. If programmes are altered, it is generally impossible to know whether that is in response to the internal PIA process, or to the wider publicity and criticism.

System of Records

The PIA process in the United States is generally internal to a particular agency. It is tied to a model of privacy oversight (which dates from the 1974 *Privacy Act*) through the analysis of discrete systems of records for which defined agency personnel have responsibility. This issue speaks to a larger structural problem with the enforcement of privacy protection rules in all advanced industrial states. How can responsibility for the processing of personal information be properly assigned when the larger technological and informational environment encourages a free flow of personal information across instutitonal and technological boundaries? Two challenges can be mentioned briefly.

First, there is little guidance as to how PIAs might be conducted wtihin an inter-agency framework. For example, there seems to be lack of clarity between the relationship between PIAs and the process of review when computer matching between different systems of records occurs. The comparison of different files to identify individuals who might be illegally claiming benefits, for example, is regulated under the 1988 *Computer Matching and Privacy Protection Act*, and the Data Integrity Boards established under this legislation to approve these matching programmes.

Second, there is a larger and more controversial question about the increasing reliance on commercial databases to achieve public policy goals, and whether or not reliance on existing private sector systems constitutes a "collection" of personal information under the *Privacy Act*.[50] At one level, the issue is a legal one. At another level, it must be noted that the institution of PIA methodology in the US has taken place within the context of a wider debate about the increasing tendency of the US government to rely on commercial

[47] Jim Dempsey, Statement, February 10, 2004.
[48] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf.
[49] Programmes such as Secure Flight, the Automated Targeting System, the U.S. Visit Program and the Trusted Traveler program.
[50] Jim Dempsey, Statement, February 10, 2004.

databases for a range of policy goals, and the consequent concerns about wider trends towards ever more extensive and intrusive methods of surveillance.[51]

Conclusion

The statutory mandate for the conduct of PIAs in the US produces some peculiar conditions and incentives which cannot translate to the UK context. Furthermore, the absence of the equivalent institution to the ICO, means that the larger questions about external review of PIAs by a privacy oversight agency cannot really be addressed in the US context. However, this brief review underlines the importance of publication, and it does suggest the need for procedures for external stakeholder consultation, at least for PIAs on major projects. Most especially, the American experience emphasises the significance of internal and institutionalised privacy expertise which can use the PIA methodology to inject privacy reasoning into internal agency deliberations at the earliest stages of decision-making and for the entire life-cycle of the project. At the end of the day, however, PIAs are only as good as the standard to which they are being conducted. In the US, that standard is principally the *Privacy Act* of 1974, a statute that for many years has been regarded as outdated, permissive of too many exemptions and "routine uses," unable to provide meaningful remedies and redress for individual citizens, and insufficiently sensitive to the realities of contemporary data processing.[52]

Research

The following individuals were interviewed:

Department of Homeland Security (practitioner):

- Rebecca Richards, Director of Privacy Compliance

Center for Democracy and Technology (privacy advocate):

- Ari Schwartz, Deputy Director

In addition, a number of primary and secondary sources were consulted, as indicated in footnotes.

[51] See for example the arguments in Daniel Solove, *The Digital Person* (New York: NYU Press, 2005), pp. 168-75.
[52] Among others, see Solove, *The Digital Person,* pp. 136-8; Robert Gellman, "Does Privacy Law Work? in Agre and Rotenberg eds. *Technology and Privacy,* pp. 193-218; David H. Flaherty, *Protecting Privacy in Surveillance Societies,* pp. 359-61.

APPENDIX E

Jurisdictional Report for Australia

CONTENTS

Context

Australia is a federation of six States and two Territories. The federated nation is formally referred to as a 'Commonwealth' and the adjective used is either 'Commonwealth' or 'Federal'.

Each of the 9 jurisdictions has responsibility for its own public sector. Regulation of the private sector in respect of consumer interests is largely performed by the States and Territories under the 'Fair Trading' banner. For the most part, however, any regulation relevant to privacy is incidental rather than intentional. Some have, however, passed privacy laws that impinge upon both the public and private operators in the health care sector.

Each of the 9 jurisdictions has responsibility for its own public sector, but constitutional powers in relation to the private sector are somewhat complex. The Commonwealth has acted in respect of the private sector generally, and the States and Territories have accepted that jurisdictional claim. Some have, however, passed privacy law in respect of the health care sector, which intersects and may conflict with the federal law.

The remainder of this document is structured into sections for the federal government and each of the six States and two Territories, in the conventional sequence of largest-first.

Research

The report has been compiled from the author's knowledge and considerable archival data, the resources provided by the Australian Privacy Commissioner and the Australian Privacy Foundation, information provided by the relevant organisation in each jurisdiction, and research using the Web.

Resources include:

"Privacy Protection Agencies", Australian Privacy Foundation.
Privacy Laws: States and Territories of Australia, Australian Privacy Foundation; and "State and Territory Privacy Laws", Office of the Privacy Commissioner of Australia.[1]
This report reflects research variously conducted and updated during July 2007, including interactions with the Commissioners or their nominees in Victoria, N.S.W. and the Northern Territory, with the Tasmanian Ombudsman, with the Privacy Committee of South Australia and with the Human Rights Unit of the Australian Capital Territory's Department of Justice and the Attorney-General.

[1] at respectively: http://www.privacy.org.au/Resources/Contacts.html#GovP, http://www.privacy.org.au/Resources/PLawsST.html and http://www.privacy.gov.au/privacy_rights/laws/.

I. Australia, Federal Government

Context

This report reflects research variously conducted and updated during July 2007, including an interview with the Australian Privacy Commissioner's nominee, Andrew Solomon, Director of Policy.

Legislative and Policy Framework

Legislation

In 1988, the *Privacy Act* (Cth)[2] was passed, to regulate the federal government public sector.

In 2000, substantial amendments were passed, applying a somewhat different regime to the private sector.

The 1988 Act created a statutory appointment called the Privacy Commissioner, supported by the Office of the Federal Privacy Commissioner (OFPC).[3]

Privacy Impact Assessment (PIA) Guidance Material

The Office released a *Privacy Impact Assessment Guide* for Australian Government and Australian Capital Territory Government agencies in 2006[4].

The Guide was devised so as to provide a brief, high-level overview, and a sense of the main methodology, but with 'drill-down' features such as checklists, in order to ensure it is sufficiently comprehensive. Key features of the Guide are outlined in Appendix 1.

The Guide was designed as guidance for government agencies. However, it is considered by the OFPC to be readily adaptable to apply to private sector companies, and the Office intends to do this, subject to resource availability.

There is no legal obligation on either government agencies or corporations to conduct PIAs (although, as discussed below, that may be changing). It is merely a Commissioner Recommendation. The Commissioner's communications with agencies and the private sector routinely contain segments of text along the following lines: 'The Office suggests that a privacy impact assessment be undertaken as part of the further development of the proposal'.

The Australian PIA

History and Development of the Australian PIA

As early as 1990, there was a clear predecessor to the concept of a PIA in the form of the 'Program Protocol' applied to data matching programmes. The then Commissioner, Kevin O'Connor, the then Deputy Commissioner, Nigel Waters, were successful in submitting to the Parliament that a particularly large 'Parallel Data Matching Program' needed to be subject to a statutory requirement to undertake a prior, justificatory study, and document the specifications for the programme.

---

[2] http://www.austlii.edu.au/au/legis/cth/consol%5fact/pa1988108/

[3] Learn more about the Commissioner and the Office at http://www.privacy.gov.au/ and http://www.privacy.gov.au/about/index.html.

[4] August, 2006. The Guide is available at http://www.privacy.gov.au/publications/pia06/index.html

The requirements of the 'Program Protocol' are declared in Schedule 1 to the Data-Matching Program (Assistance and Tax) Act 1990,[5]

Building on the 1990 'Program Protocol', the then Commissioner, Kevin O'Connor, published Guidelines for 'Data-Matching in Commonwealth Administration' (June 1992). These are not legally binding, but it was recommended that all agencies conduct such an assessment when considering undertaking any form of data matching. The current version is dated February 1998.[6]

The earliest mentions of the term 'PIA' found in Australian sources appear to be the following:

- a 1995 acknowledgement by the Telecommunications Industry Ombudsman that PIAs had a role to play (referred to in the 1997 paper discussed below);
- 1996 papers by Blair Stewart (New Zealand's Deputy Privacy Commissioner), in Privacy Law and Policy Reporter;[7]
- a 1997 call by the Communications Law Centre for implementation of PIAs, invoking Blair Stewart's definition as "a process whereby a conscious and systematic effort is made to assess...any actual or potential effects that [an] activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated" and referring also to David Flaherty's work in British Columbia; [8] and
- papers of Roger Clarke in 1997-99.[9]

In December 2001, the then Commissioner, Malcolm Crompton, issued 'Guidelines for Agencies using PKI to communicate or transact with individuals':[10] These included as Guideline 3:

> "Agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI system".[11]

A PIA was depicted as "a method of identifying privacy risks so that these can be highlighted and addressed when ... systems or ... business applications are being designed, implemented, revised or extended. A PIA may be part of a larger risk assessment and management procedure. Properly done, this assessment will include an understanding of which parties will bear what risks".[12]

It was expressly stated that "agencies should provide their clients with anonymous and pseudonymous options for transacting with them, to the extent that this is not inconsistent with the objectives and operation of the relevant online application"[13]

---

[5] at: http://www.austlii.edu.au/au/legis/cth/consol_act/dpata1990349/index.html and http://www.austlii.edu.au/au/legis/cth/consol_act/dpata1990349/sch1.html.
[6] at: http://www.privacy.gov.au/publications/dmcomadmin.pdf.
[7] at http://www.austlii.edu.au/au/journals/PLPR/1996/39.html and http://www.austlii.edu.au/au/journals/PLPR/1996/65.html.
[8] at http://www.austlii.edu.au/au/journals/PLPR/1997/4.html
[9] at http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.htmland in greater depth at http://www.xamax.com.au/DV/PIA.html.
[10] at: http://www.privacy.gov.au/publications/pki.doc
[11] 'Guidelines for Agencies using PKI to communicate or transact with individuals' p. 29
[12] p. 35.
[13] (Guideline 9, p. 35).

Further guidance was provided on pp. 36-38 (referencing Blair Stewart's work in New Zealand), and a customised checklist for Information Privacy Principle compliance on pp. 39-43.

In January 2003, in a Submission to the Joint Committee of Public Accounts and Audit (JCPAA) on 'Management and Integrity of Electronic Information in the Commonwealth', the then Commissioner, Malcolm Crompton, stated:

> "Recommendation 2 – that Commonwealth agencies be required to undertake privacy impact assessments at the beginning of the development of new proposals and initiatives involving the handling of the personal information of the Australian community.[14]
>
> "These assessments should be published unless national security or law enforcement considerations outweigh the public interest in the publication. If an assessment is not to be published, it should be copied to the Privacy Commissioner, the Attorney-General's Department; the Department of Finance and Administration and the Department of Prime Minister and Cabinet."[15]
>
> and
>
> "Recommendation 3 – that the Cabinet Handbook and the Department of Prime Minister and Cabinet's Drafter's Guide be amended to more specifically guide agencies in their early assessment of the privacy impact of new proposals relevant to Cabinet Submissions, Cabinet Memoranda and like documents".[16]

In November 2004, the Commissioner, Karen Curtis, issued an Exposure Draft of 'Managing Privacy Risk: An Introductory Guide to Privacy Impact Assessment'. The draft was based on considerable research into the experiences of and guidance provided in other jurisdictions, particularly New Zealand, Canada and Ontario. Comment was invited from the public and privacy advocacy groups:[17]

Among other submissions, the Australian Privacy Foundation suggested a number of enhancements. [18]

In August 2006, the final version of the 'Privacy Impact Assessment Guide' was released.[19]

In launching the Guide, the Attorney-General said, "as a matter of good business practice, I strongly encourage government agencies to use the guide to assist them in playing a larger role in promoting privacy compliance".[20]

Completion of PIAs

---

[14] Malcolm Crompton, Submission to the Joint Committee of Public Accounts and Audit (JCPAA) on 'Management and Integrity of Electronic Information in the Commonwealth', at pp. 19-20 of: http://www.privacy.gov.au/publications/jcpaasubs.doc

[15] Ibid, section 3.1.5.1

[16] Ibid.

[17] See Office of the Privacy Commissioner of Australia Media Release, *Announcement: Draft of Managing Privacy Risk - An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies*, at: http://www.privacy.gov.au/news/04_07.html

[18] at: http://www.privacy.org.au/Papers/OFPC-PIA-0502.rtf

[19] at: http://www.privacy.gov.au/publications/pia06/toc.html and http://www.privacy.gov.au/publications/PIA06.doc and http://www.privacy.gov.au/publications/PIA06.pdf.

[20] at: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2006_Third_Quarter_29_August_2006_-_Speech_-_Privacy_impact_assessment_guide_and_layered_privacy_policy_launch

By Which Organisations?

The Privacy Commissioner's 2006 Guide is specifically addressed to government agencies.

PIAs are performed for a wide range of purposes in a wide range of contexts. One particular PIA project utilised several specific features that have the potential to offer considerable payback. Centrelink is the delivery channel for about 100 benefits programmes run by various Australian government agencies. It provides services to over 20% of the Australian population, many of them on a regular basis.[21] The effectiveness and efficiency of Centrelink's business processes are heavily dependent upon use of technology in a manner that works for both the agency and its clients. Automated authentication of clients' voices over the telephone offers considerable promise, but brings with it risks that are not easy to grasp and to articulate.

A number of recent developments show that the Commissioner's 'moral suasion' is having considerable impact:

- since March 2005, the Australian Government Information Management Office (AGIMO – called in other jurisdictions the Office of the Government CIO) has specifically pressed for a PIA to be done in relation to **authentication projects more generally;** [22]
- in June 2006, AGIMO extended the authentication work to the Australian Government Smartcard Framework;[23]

  This requires that "**One or more Privacy Impact Assessments should be undertaken at critical points during the design and rollout of the smartcard solution**, such as at initial design, final design, and whenever a significant change occurs to the deployed system, such as third party agency deciding it may wish to re-use the initial deployment. This is **consistent with the Australian Government e-Authentication Framework**";[24]
- in July 2006, the Privacy Commissioner approved a Biometrics Code prepared by an industry association, the Biometrics Institute.[25] This includes **a requirement for privacy impact assessments as part of the planning and management process for biometrics implementations, which is the first context in which any form of statutory mandation has arisen.** (However, because the code is voluntary and there are virtually no signatories to it, the mandation is currently not meaningful);

[21] at: http://www.centrelink.gov.au/.
[22] See the 'Australian Government Authentication Framework for Business, Part 5 – Evaluating the business, privacy and public policy impacts', at http://www.agimo.gov.au/infrastructure/authentication/agaf_b/impguidegovt/volume3/part5
[23] at: http://www.agimo.gov.au/infrastructure/smart_cards and http://www.agimo.gov.au/__data/assets/pdf_file/56247/Overview_and_Principles_PUBLISHED_June2006.pdf and http://www.agimo.gov.au/__data/assets/pdf_file/56248/Smartcard_Handbook_PUBLISHED_June2006.pdf
[24] fn. 23 at p. a17
[25] at: http://biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8 http://biometricsinstitute.org/associations/4258/files/2006-07%20Biometrics%20Institute%20Privacy%20Code%20approval%20determination%20FINAL.doc

- in April 2007, **the head of the Attorney-General's Department wrote to all agency heads** on privacy issues generally, extolling the benefits of using PIAs early in the project life-cycle;
- **some agencies have implemented internal programmes to apply PIAs**, integrating them with related areas of responsibility. An example is the Department of Defence's 'Fairness and Resolution' Programme;[26]
- since the Guide was launched in August 2006, there have been **23,000 hits or downloads**, with spikes following events such as meetings with agency Privacy Contact Officers (PCOs). Although the OFPC is not directly involved in agency activities, the impression gained by the OFPC is that the Guide is being used quite extensively. It is common for Requests for Tender for consultancy support for PIAs to explicitly require that the Commissioner's Guide be at least reflected, and in most cases complied with. On the other hand, PIAs are not yet performed as a matter of course, even within Government, and even for projects with significantly privacy-invasive features.

Examples of PIAs known to have been conducted by federal agencies include are in Appendix 1.

Examples of PIA Reports known to have been published are listed in Appendix 2.

Private Sector PIAs

There is some degree of application in the private sector, but it is not widespread, and few PIAs have been widely publicised. Whereas the public sector uses the terms 'compliance check', 'privacy notices', 'PIA' and 'privacy audit', the terminology applied in the private sector includes 'privacy strategy', 'privacy (management or implementation) plan', 'privacy policies', 'privacy statements' and 'privacy review'.

In March 2005, the Commissioner, Karen Curtis, published a review of the private sector provisions of the *Privacy Act*. In s.8.4, 'Options for reform', the Report referred to:

> "Promote privacy impact assessments and privacy enhancing technologies: ... **"**The Office could encourage technology developers and implementers to conduct a privacy impact assessment for large scale high privacy risk projects. A wider review of the *Privacy Act* could consider the question of whether the Privacy Act should include provisions which provide for a privacy impact assessment to be carried out in specified circumstances."[27]

It is understood that in 2006 Coles-Myer[28] adapted the Commissioner's PIA Guide to reflect the private-sector National Privacy Principles (NPPs) rather than the public-sector Information Privacy Principles (IPPs), and applied them to a project to produce a customer data warehouse.

Examples of PIAs known to have been conducted in the private sector, in public-private partnerships, or otherwise with considerable private sector involvement are listed in Appendix 3.

Who Writes and Participates in Development of PIAs?

[26] at: http://www.defence.gov.au/fr/ and http://www.defence.gov.au/fr/Privacy/privacyimpact.htm
[27] (pp. 255-256) http://www.privacy.gov.au/act/review/revreport.pdf.
[28] Australia's largest retailer, with more than 1900 stores throughout Australia and New Zealand, at: http://www.colesgroup.com.au/Home/.

The Guide proposes that agencies adopt a team approach, using 'in-house experts' and outside expertise as necessary. In practice, there has been considerable use of the small number of specialist consultants with expertise in the area.

When?

The Guide implies that PIAs should be commenced early, in order to shape the evolution of the project. It provides only limited guidance as to how to assess when a PIA is needed. It does, however, refer to "significance", "size", "complexity" or "scope", the extent to which the project involves "collection, use or disclosure of 'personal information'", both in general, and particularly "information that is generally regarded as sensitive".

External Consultation

Centrelink formed a PIA Consultative Group (PCG), comprising representatives of people in various client segments, together with advocates for consumer and privacy interests. Project staff provided background information and briefings to the PCG, enabling members to surface and articulate concerns. By working with such a group, an agency's officers can achieve much deeper insight into the project's likely negative impacts, and what can be done to avoid or ameliorate them. In extreme cases, advance warning could be gained of serious public sensitivities.

The PCG was called together in several successive phases of the project. Briefings became shorter and conversations more tightly focused. The confidence of the PCG members in the agency's goodwill was greatly increased as they found that the subsequent phases were clearly reflecting the outcomes of earlier rounds.

Another approach adopted by Centrelink (in a project to develop an 'authentication hub' to enable single sign-on to multiple agencies) was to expose the design to people from various client segments who would be affected by the project. Consumer/citizens are seldom able to discuss abstract ideas, so a prototype was essential to enable this form of consultation to be effective. Deeper understanding about people's views and reactions can be gained by drawing the invitees into focus groups.

These approaches to consultation contribute significantly to risk reduction in complex IT projects. Feedback is captured at multiple stages in the process, which underpins an adaptive approach to system design and avoids new systems being 'legacy systems' even before they are implemented.

Review/Approval of PIAs

The OFPC drew attention to a risk inherent in mandation. Organisations might focus on compliance rather than adopting a strategic approach, and might therefore fail to gain the benefits that are available from appropriately open and imaginative processes. This makes it all the more important for agencies and corporations to be themselves responsible for devising an appropriate process, rather than being subject to overly prescriptive dictates by the Parliament or the Privacy Commissioner.

Public Availability

The Guide envisages that PIA Reports will generally be published. A few have been. See Appendix 3.

Lessons Learned

A number of areas of weakness in PIAs has been commented on by participants and observers. There remains a tendency for agencies to confuse a PIA with a check of compliance with the provisions of the *Privacy Act* or even just the Information Privacy Principles. The use of the small number of consultants with specialist expertise tends to result in PIA processes with broader scope and better ability to deliver benefits to the agency and its clients alike.

The mapping of information flows relevant to privacy impacts has proven to be challenging in some contexts. The documentation needs to be sufficiently full and clear, but also accessible, and this requires skill and effort.

A common shortfall has been a failure to define 'stakeholders' so as to encompass the people affected by the project, and to involve them and/or their representatives and advocates in the PIA process.

Finally, depending on the nature of the project, the scope of a PIA may need to extend beyond information privacy to encompass other dimensions, including privacy of the person (e.g. proposals for the imposition of biometric measurements), privacy of personal behaviour (e.g. visual surveillance) and privacy of personal communications. There may also be benefits for the agency (both in terms of cost-savings and benefit-enhancement) in extending the scope to other social impacts. such as equity, accessibility, anti-discrimination and occupational health and safety.

Directions of PIAs in the Jurisdiction

At this early stage, there has been no formal review of the 2006 Guidelines or their application. The OFPC is, however, looking to review and enhance the Guide during 2008, in what may be by then a somewhat different context. It is not seeking to move towards an approval model, believing that the most effective role it can play is to provide a framework, methodology and tools, and be available to provide high-level advice and review of agencies' PIA plans, while ensuring that the effort is invested (and the benefits are gained) by the organisation sponsoring the project.

In March 2005, the Commissioner's Review of the private sector provisions of the *Privacy Act*, included,[29]

Recommendation 1: The Australian Government should consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia" [30]

Partly in response to that Recommendation, the **Senate Legal and Constitutional References Committee** held an Inquiry into the Privacy Act during the first half of 2005. Several organisations submitted that PIAs should become a requirement under particular circumstances, including the Victorian Privacy Commissioner, the Law Institute of Victoria, the Australian Privacy Foundation, and Electronic Frontiers Australia.

The Committee's Report expressed concern generally, and about several particular projects that used advanced information technologies or were otherwise highly privacy-intrusive. It considered that **"it is possible update the Privacy Act in a 'technology neutral' way to reflect the technological changes that have occurred and to enable the Privacy Act to deal with these new technologies"**. It made general and specific Recommendations to address the situation, including:

Recommendation 5

[29] at: http://www.privacy.gov.au/act/review/revreport.pdf.
[30] At p. 8.

> 7.13 The committee recommends the Privacy Act be amended to include **a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information**.

Relevant excerpts from the Senate Committee's Report are provided in a companion document.

In January 2006, partly as a consequence of the Senate Committee's Recommendations, the Attorney-General provided terms of reference to the Australian Law Reform Commission to conduct a Review of the operation of the *Privacy Act*.

In October 2006, the Commission published a substantial Issues Paper, which discussed the question of PIAs, and asked the following specific questions:

> **Question 6–6:** Should the *Privacy Act* require a privacy impact assessment to be prepared for:
>
> (a) all proposed Commonwealth legislation;
>
> (b) other proposed projects or developments of agencies; or
>
> (c) other proposed projects or developments of organisations?
>
> **Question 6–7:** If privacy impact assessments are required:
>
> (a) who should be involved in preparing the assessments;
>
> (b) who should be entitled to view the results of the assessments;
>
> (c) who should bear the cost of the assessments; and
>
> (d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

Relevant excerpts from the Issues Paper are provided in a companion document.

A number of Submissions are known to have been made in response to these questions, and it is generally assumed that agencies and industry associations may have made Submissions as well, which the ALRC does not publish and which the organisations concerned may well not publish either.

In March 2007, in the Executive Summary of the Commissioner's Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31, the Commissioner recommended that "public sector agencies be required to undertake Privacy Impact Assessments for new projects or legislation that significantly impact on the collection or handling of personal information".

More specifically, the Privacy Commissioner submitted, “The Office supports the introduction of a statutory requirement on public sector agencies to undertake a Privacy Impact Assessment (PIA) for new projects and/or legislation that significantly impact on the collection or handling of personal information. This should include:

- a set of criteria to establish when a PIA is required;
- an appropriate regulatory mechanism to ensure compliance.

2. The Office does not believe a mandatory requirement should be imposed on private sector organisations to undertake a PIA. However, organisations should be encouraged to undertake a PIA for large scale, high privacy risk projects.

3. **The Office should develop PIA guidelines tailored for the needs of the private sector through consultation**." [31]

Trends

In interview, the OFPC felt that momentum towards more widespread use of PIAs was building, in both the public and private sectors.

[31] at: http://www.privacy.gov.au/publications/submissions/alrc/exec.html#Question44

Appendix 1: Key Features of the Australian PIA Guide

- It is specifically **addressed to government agencies**. The Privacy Commissioner has separately flagged the need for, and the intention to deliver, PIA Guidelines for the private sector;
- It introduces the concept of a PIA by saying it "**'tells the story' of a project or policy initiative from a privacy perspective** and helps to manage privacy impacts" (p. 4), and ascribes that depiction to David Flaherty;
- It defines a PIA as "**an assessment tool** that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals" (p. 4) – re Q3;
- It frames the purposes of doing a PIA, and the benefits arising from it, in terms of **the assistance a PIA can provide to agencies**. The approach is well summed up by the catch-phrase "The PIA pay off: helping to ensure the success of the project" (pp. 4-5, 7);
- It stresses the **risk management aspects** of a PIA (pp. 5-7), and in doing so refers to the relevant section of the Ontario Guidelines (1999, pp. 15-16);
- It **clearly distinguishes a PIA from privacy law compliance**, referring to the need for the agency to consider the "values the community places on privacy – trust, respect, individual autonomy and accountability – and to reflect those values in the project by meeting the community's privacy protection expectations" (pp. 5-6) – re Q3;
- It focusses on **process rather than product**: "A PIA works most effectively when it forms part of a project's development, so that it helps to shape the evolution of the project. This ensures that privacy is 'built in' rather than 'bolted on';
- "Given the importance of a PIA in the evolution of a project involving personal information, the PIA document itself will also usually tend to be an evolving or living document. ... **Projects which are more significant in scope may even require more than one PIA throughout their development**" (p. 7);
- It asks the question "Is a PIA Necessary?", and refers to '**Threshold Assessment**' (p. 10). The Privacy Commissioner provides only limited guidance as to how to assess that Threshold, but it does refer to "significance", "size", "complexity" or "scope", the extent to which the project involves "collection, use or disclosure of 'personal information'", both in general, and particularly "information that is generally regarded as sensitive" (p. 8) – re Q4;
- It proposes **"a team approach"**, using "various 'in-house experts'" and "outside expertise as necessary". "In many cases, a set of 'fresh eyes' looking over a project can identify privacy impacts not previously recognised" (p. 8) – re Q5;
- "It will often be appropriate to consult widely. **Consultation with key stakeholders is intrinsic to the PIA process** as it helps to ensure that key issues are noted, addressed and communicated. As a PIA also involves consideration of community attitudes and expectations in relation to privacy, and because potentially affected **individuals are likely to be key stakeholders, public consultation will also often be important**" (p. 9) – re Q6;
- "The PIA should **feed into** further planning about the project's next steps", including resource allocation, stakeholder management, advising Ministers and

government (including about risks), staffing, **the design of the scheme**, trialling, testing, consultation, public education and evaluation (p. 17);

- It envisages that the results, in the form of **the PIA Report, will be published** (p. 17) – re Q7. In interview, the OFPC noted that, where a multi-phase PIA process is conducted, there may be advantages in early documents not being published, in order to help discussions to be open, and ideas to 'gel';
- Guidance is provided in relation to the **conduct of the PIA**:
  - project description (p. 13 and Module B);
  - mapping the information flows (p. 14 and Module C);
  - privacy impact analysis (pp. 15-16 and Module D);
  - Information Privacy Principle compliance (Module E);
  - privacy management, recommendations, implementation, and post-implementation review (pp. 16-17 and Module F);
- Because the statute does not mention PIAs, and the Office is not resourced to provide anything more than general assistance to agencies, **the Privacy Commissioner has no formal role** in the development, endorsement or approval of PIAs (p. 17) – re Q5, Q8;
- "It is important to note ... that, whilst information privacy is the regulatory focus of the Office and this Guide, it is only one aspect of privacy more broadly. For example, there are other types of privacy (such as bodily privacy; territorial privacy; communications privacy).1 **Whilst this Guide is primarily designed to address information privacy issues through the PIA process, other types of privacy can also be considered, particularly where such privacy issues may pose risks to the overall success of the project**" (p. 3).

Appendix 2: Examples of PIAs by or for Australian Government Agencies

- National E-Health Transition Authority (NEHTA), re a unique health identifier (2006-07)
- Access Card Privacy and Consumer Task Force, re a proposed national identification scheme (2006-07)
- Attorney-General's Department, re Document Verification Service (DVS, 2007)
- Attorney-General's Department, re AusCheck – employee background checking services for the maritime and aviation industries (2007)
- Centrelink (the government benefits administrator), re a voice authentication scheme to be implemented within the IVR application on the (very) high-volume call centre (2005, 2006, 2007)
- Australian Communications and Media Authority (ACMA), re ENUM (a scheme to enable mapping between telephone numbers and Internet IP-addresses (2006)
- Attorney-General's Department, re provisions within the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules (AML-CTF, 2006)
- Department of Health, in relation to Electronic Health Records (2006)
- Australian Government Information Management Office (AGIMO), re the Australian Government Authentication Framework (AGAF, 2004, 2005, 2006)
- Australian Government Information Management Office (AGIMO), re the Gatekeeper PKI Framework (2006)
- Department of Human Services, re a common login-point for multiple client-facing agencies (2006)
- Attorney-General's Department, re provisions within a money-laundering / counter-terrorism Bill (2006)
- Department of Human Services, re a proposed ID card for clients of a variety of agencies (2005)
- Department of Employment & Workplace Relations, re Workplace Reform (2005?)
- Department of Education, Science & Training, re a Learner Identity Management Framework, a Commonwealth-State collaboration featuring a unique student identifier (2005)
- Australian Bureau of Statistics (ABS), re enhancements to the 2006 Census (2005)
- Department of Health, re electronic consent (2004)
- National Office of the Information Economy (NOIE), re the Australian Government Authentication Framework (AGAF, 2003)
- Centrelink, re a proposed ID card for Centrelink clients (1998)
- Department of Workplace Relations and Small Business, re a business register (1998)
- Australian Commission for the Future, re smartcard payment schemes (1996)

Appendix 3: Examples of Published PIA Reports by or for Australian Government Agencies

- NEHTA Unique Health Identifier (Privacy 'Blueprint' rather than PIA), at http://www.nehta.gov.au/index.php?option=com_docman&task=doc_details&gid=148

- Attorney-General's Department, re Document Verification Service (DVS, 2007), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(756EDFD270AD704EF00C15CF396D6111)~FINAL+PIA+for+publication+on+webpage+-+June+2007.pdf/$file/FINAL+PIA+for+publication+on+webpage+-+June+2007.pdf

- Attorney-General's Department, re AusCheck – employee background checking services for the maritime and aviation industries (2007), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(756EDFD270AD704EF00C15CF396D6111)~Privacy+Impact+Assessment+-+Auscheck.pdf/$file/Privacy+Impact+Assessment+-+Auscheck.pdf

- Attorney-General's Department, re provisions within the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules (AML-CTF, 2006), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~88Privacy+impact+assessment+aml-06.pdf/$file/88Privacy+impact+assessment+aml-06.pdf

- Australian Government Information Management Office (AGIMO), re the Gatekeeper PKI Framework (2006), at http://agencysearch.australia.gov.au/search/click.cgi?url=http://www.agimo.gov.au/__data/assets/pdf_file/52237/Galexia_Privacy_Impact_Assessment.pdf&rank=3&collection=agencies

- Australian Bureau of Statistics (ABS), re enhancements to the 2006 Census (2005), at www.abs.gov.au/websitedbs/D3110124.NSF/f5c7b8fb229cf017ca256973001fecec/fa7fd3e58e5cb46bca2571ee00190475!OpenDocument

Appendix 4: Examples of Private Sector PIAs

- Coles-Myer, re a customer data warehouse (2006)
- Telecommunications, specifically ENUM, undertaken by a Working Group coordinated by the regulator (ACMA), but also involving industry associations and some technology providers (2006)
- An identity management service (Fasfind, 2004)
- Transport ticketing (Melbourne myki, 2004)
- Forensic applications of an email archive analysis product (Nuix, 2002)
- A PKI certificate authority for the health sector (Healthexchange, 2000)
- Toll-roads (Melbourne CityLink, 1998)

Appendix 5: Senate Legal and Constitutional References Committee Inquiry into the *Privacy Act* 1988

Context

In December 2004, the Legal & Constitutional References Committee of the Australian Senate was given a reference to conduct a Review Of The *Privacy Act* 1988:
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/tor.htm

The 49 published Submissions are at:
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/submissions/sublist.htm

In June 2005, the Committee published its Report, entitled 'The real Big Brother: Inquiry into the *Privacy Act* 1988'. The document is at:
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/index.htm
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/report.pdf
(800KB)

This document identifies all parts of the text that use the term 'privacy impact assessment', and provides excerpts of them. Segments of particular significance are highlighted in bold-face type.

Excerpt 1

Privacy impact assessments (p. 21-22)

3.25 **Another suggestion put forward in submissions [by the Victorian Privacy Commissioner] was that privacy impact assessments should be conducted prior to the implementation of new technologies.34 The APF submitted that privacy impact assessments are now a mandatory requirement in several jurisdictions including the USA and Canada. Criteria should be developed, drawing on international experience, for triggering such a requirement under the *Privacy Act*. PIAs [Privacy Impact Assessments] should be conducted by independent assessors but paid for by scheme proponents, with the Privacy Commissioner setting and monitoring appropriate standards**.35

3.26 Similarly, **the LIV [Law Institute of Victoria] suggested that government agencies and organisations should be required to prepare a privacy impact assessment if they propose to apply new technologies in a way that entails collecting more information than before, sharing it more freely than before, using existing or new information for new purposes not envisaged before, or holding it longer than before. If the Privacy Impact Assessment reveals significant risks in the view of the Privacy Commissioner, further regulation could be required, whether it be a code, regulations or new legislation**. 36

3.27 The LIV continued: We suggest that Privacy Impact Assessments will introduce a process under which due consideration should be given to the privacy rights of individuals in the context of other public interests, such as national security, law enforcement and administrative efficiency. Without a predictable, structured process to assess the privacy implications of proposals that could have a broad and significant impact on the community, each new idea is likely to attract controversy and criticism until the necessary analysis has been done.

3.28 Mr Bill O'Shea from the LIV elaborated on this during the Committee's hearing in Melbourne, suggesting that there are various ways such privacy impact assessments could be done: For example, if Medibank Private or Medicare were to change the way they collect information on behalf of members we would expect that an impact

statement as to what that change would be would be provided to all members. If that were to go through parliament we would expect that impact statement to be part of the legislation, certainly either incorporated in the second reading speech or made available to the public. ...If there were other examples where legislation was not required, we would expect the peak body for the organisation that had that information to provide a privacy impact assessment for those people in the public who were dealing with it. If, for example, it involved the Insurance Council of Australia we would expect to be required to produce for the public a privacy impact assessment of whatever they were planning to do.38

3.29 Ms Irene Graham from **EFA expressed qualified support for the concept of privacy impact assessments, but cautioned that if the OPC were to conduct the assessments, funding and resourcing issues would need to be addressed**.39

3.30 The OPC acknowledged that it encouraged the use of privacy impact assessments: We have advised that [government] departments should consider a privacy impact assessment process whereby they examine any new policy proposal in the light of the impacts on a person's privacy, and that, each step along the way, they should continuously look to see what it is they are proposing to do and whether it is the best way. Things can be done in a privacy-enhancing way rather than in a privacy-intrusive way. As we often say, the biggest invasion of a person's privacy is that their identity is stolen, so we need to address some of those issues.40

3.31 **It is also noted that the OPC is developing privacy impact assessment guidelines for public sector agencies, which the OPC considers could also be applicable in the private sector**.41 The OPC also noted that 'a wider review of the *Privacy Act* could consider the question of whether the *Privacy Act* should include provisions which provide for a privacy impact assessment to be carried out in specified circumstances.'42

32 Submission 47, p. 4 cf EFA, Submission 17A, pp 7-8.

33 Submission 47, p. 4.

34 See, for example, Office of the Victorian Privacy Commissioner, Submission 33, p. 5; LIV, Submission 37, p. 5; APF, Submission 32, p. 11.

35 Submission 32, p. 11.

36 Submission 37, pp 6-7.

37 Submission 37, p. 7.

38 Committee Hansard, 22 April 2005, p. 16.

39 Committee Hansard, 22 April 2005, pp 45-46. Note also that the issue of funding and resourcing of the OPC is discussed in further detail later in this report.

40 Committee Hansard, 19 May 2005, p. 55.

41 OPC review, p. 256.

42 OPC review, p. 256.

Excerpt 2

Medicare smartcard (p. 30)

3.59 **EFA suggested that, at the very least, an independent privacy impact assessment of the smartcard should be conducted**, and that security measures should be built into the smartcard.86

86 Submission 17, p. 24.

Excerpt 3

Biometric Passports (p. 36)

3.81 **In response to the committee's questioning on to the extent to which privacy impact assessment had been, or was being, conducted in relation to the biometric passports, a representative of DFAT replied: There have been two privacy impact assessment projects conducted so far**. One was done prior to the introduction into parliament of the legislation. That was done last year. That privacy impact assessment of course included the provisions relating to the introduction of biometric technology into Australian passports. And there is currently a biometrics- or e-passports- specific privacy impact assessment being prepared.126

3.82 The representative noted that the assessment was being prepared 'internally in consultation with privacy advocates and the Privacy Commissioner'.127

3.83 Indeed, the OPC noted that it had provided advice on the passports legislation, and that this advice had been 'taken on board'.128 Further, it was noted that **the Privacy Commissioner had been funded in the recent budget 'to work with Customs and DIMIA [Department of Immigration and Multicultural and Indigenous Affairs] and DFAT on biometrics**.'129

3.84 However, EFA advised that they believed that any privacy protection afforded by the *Privacy Act* in this context was likely to be 'weak at best'. In particular, EFA was concerned that any disclosure pursuant to a determination made by the Minister under the Passports Act would be 'authorised or required by law' and therefore fall within the category of disclosure to which the *Privacy Act* does not apply.130

3.85 Some submitters were also concerned that the chip to be implanted in passports could be read remotely, and that this could actually facilitate identity theft.131 For example, Mr Roger Clarke described the passports proposal as 'naïve and dangerous', arguing that placing enormously sensitive data into an RFID tag, including biometrics will facilitate identity theft.132

125 Submission 39, p. 4.

126 Committee Hansard, 20 May 2005, p. 2.

127 Committee Hansard, 20 May 2005, p. 2.

128 Mr Timothy Pilgrim, OPC, Committee Hansard, 19 May 2005, pp 55-56.

129 Ms Karen Curtis, OPC, Committee Hansard, 19 May 2005, p. 55.

130 Submission 17, p. 29.

131 EFA, Submission 17, pp 27-28; Mr Roger Clarke, Submission 28, p. 2.

132 Submission 28, p. 2.

Excerpt 4

Census (p. 133)

5.116 However, **the committee notes that the ABS census proposal has been released for public consultation and will also be subject to a privacy impact assessment, which will also be published**.151

151 ABS, Discussion Paper: Enhancing the Population Census: Developing a Longitudinal View, ABS 2060.0, April 2005, p. 18.

Excerpt 5

Powers of the Office of the Privacy Commissioner (p. 147)

6.39 The APF submitted that the functions and powers of the Privacy Commissioner are generally adequate, but ineffective due to lack of resources. Nevertheless, **the APF recommended a number of extended or additional powers for the Privacy Commissioner, including**:

- extending the audit function to compliance by private sector organisations with the NPPs;
- the power to initiate a code of practice to deal with particular issues affecting the private sector;
- **the power to selectively require agencies and organisations to publish details of major projects or proposals with significant privacy implications**;
- **an express role in relation to privacy impact assessments**;
- the power to issue or require corrective statements; and
- a more systematic and streamlined complaints process.56

56 Submission 32, pp 23-24; pp 26-27.

Excerpt 6

A comprehensive review (pp. 151-152)

Recommendation 1

7.4 **The committee recommends that the Australian Government undertake a comprehensive review of privacy regulation**, including a review of the *Privacy Act* 1988 in its entirety, with the object of establishing a nationally consistent privacy protection regime which effectively protects the privacy of Australians.

Recommendation 2

7.5 **The committee recommends that the Australian Law Reform Commission undertake the review** proposed in recommendation 1 and present a report to Government and to Parliament.

Excerpt 7

Emerging technologies (p. 153)

7.10 The committee is particularly concerned that the *Privacy Act* is simply not keeping up with the privacy challenges posed by new and emerging technologies. While the *Privacy Act* may have been an appropriate mechanism to respond to the technologies of the 1970s and 1980s, technology has moved at a rapid pace in the past few decades, and the *Privacy Act* has not been updated accordingly. The committee considers that the introduction of other legislation to deal with the emerging technologies, such as the Spam Act 2003, is a clear demonstration of the failure of the *Privacy Act* to adequately respond to new technologies.

7.11 The committee acknowledges calls for the *Privacy Act* to remain 'technology neutral'. Indeed, the committee considers that it is desirable for the *Privacy Act* to remain as 'technology neutral' as possible. However, **the committee believes that it is possible update the *Privacy Act* in a 'technology neutral' way to reflect the technological changes that have occurred and to enable the *Privacy Act* to deal with these new technologies**.

7.12 As mentioned above, the committee proposes that the ALRC review at recommendations 1 and 2 should examine ways to improve privacy regulation to improve its capacity to respond to emerging technologies. At the same time, the committee also agrees with some of the suggestions that were put forward during this inquiry. In particular, **the committee considers that the *Privacy Act* should be amended to set out a statutory process for the conduct of privacy impact assessments in relation to new proposals which may have a significant impact on privacy. This assessment process could be a transparent and accountable way of ensuring that privacy concerns are addressed. The committee notes that privacy impact assessments are being conducted in relation to some new proposals such as biometric passports. However, the committee is concerned that these assessments are not being conducted in an open and transparent manner. The committee considers that such assessments need to involve full public consultation and should be occurring in a transparent and accountable manner**. The committee considers that the details of this statutory privacy impact assessment process could be developed by the Australian Law Reform Commission as part of the review proposed in recommendations 1 and 2.

Recommendation 5

7.13 **The committee recommends the *Privacy Act* be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information.**

Excerpt 8

Other technologies (pp. 154-55)

7.19 The committee notes the evidence received in relation to the privacy implications of smartcard technology, and that such technology can be either privacy enhancing or privacy invasive. The area of most immediate concern to the committee is the Medicare smartcard. **The committee heard evidence of the lack of wider public consultation in relation to the privacy implications of the Medicare smartcard. Indeed, the committee is disturbed that it appears that key stakeholders were not**

consulted prior to the introductory trial of the Medicare smartcard. The committee is also concerned about the potential for function creep in the use of the Medicare smartcard.

7.20 **The committee is similarly concerned about the lack of public consultation, and indeed, the lack of publicly available information, in relation to the government's proposed national document verification service.**

7.21 **The committee also acknowledges concerns raised in submissions and evidence in relation to the privacy implications of biometric technology and the proposed biometric passports. The committee also notes the evidence of DFAT that a privacy impact assessment is being prepared in relation to the proposed biometric passports, in consultation with the OPC. However, once again, the committee is concerned that the privacy impact assessment does not appear to be being conducted in a particularly open or transparent manner.**

7.22 **The committee notes with concern the recent authorisation by the US FDA of human microchip implants. However, the committee was reassured to learn from relevant government departments that there are no similar proposals currently planned here in Australia. Nevertheless, the committee considers that this is an issue that has significant privacy implications, and that such microchip implants should be properly regulated here in Australia.**

7.23 **The committee also notes the extensive list of other technologies raised in submissions to the inquiry, including, but not limited to: RFID; spyware; location-based services; electronic messaging; and other telecommunications technology. The committee considers that the ALRC review should examine the privacy implications of these technologies, and whether appropriate regulatory measures are in place to ensure that privacy is adequately protected in relation to these technologies. Such regulatory measures should also be consistent and as technologically neutral as possible.**

Recommendation 8

7.24 The committee recommends that the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2, include consideration of the privacy implications of new and emerging technologies with a view to ensuring that these technologies are subject to appropriate privacy regulation.

Appendix 6: Australian Law Reform Commission, Extracts from Issues Paper 31 re Review of the *Privacy Act*

Context

In January 2006, the Australian Law Reform Commission was given a reference to conduct a Review of the *Privacy Act* 1988:
http://www.alrc.gov.au/inquiries/current/privacy/terms.htm

In October 2006, the Commission published 'ALRC Issues Paper 31 Review of Privacy'. This is a very substantial document, designed to elicit reponses concerning a wide range of issues. The document is at:
http://www.austlii.edu.au/au/other/alrc/publications/issues/31/
http://www.austlii.edu.au/au/other/alrc/publications/issues/31/IP31.pdf (8MB)

The Commission's policy is to not publish Submissions made to it, and consequently it cannot be established with confidence what responses were provided to it, and by whom.

The Commission's Report is not due until March 2008.

This document identifies all parts of the text that use the term 'privacy impact assessment', and provides excerpts of them. Segments of particular significance are highlighted in bold-face type.

Excerpt 1

2. Overview of Privacy Regulation in Australia

Privacy impact statements and assessments

2.111 Primary legislation and delegated legislation that affect business may require the preparation of a Regulatory Impact Statement (RIS). An RIS is a document prepared by the department, agency, statutory authority or board responsible for a regulatory proposal following consultation with affected parties, formalising some of the steps that must be taken in good policy formulation. It requires an assessment of the costs and benefits of each option, followed by a recommendation supporting the most effective and efficient option. Subject to limited exceptions,[183] the preparation of an RIS is mandatory for all reviews of existing regulation, proposed new or amended regulation and proposed treaties which will directly affect business, have a significant indirect effect on business, or restrict competition.[184]

2.112 **One issue is whether a 'privacy impact statement' should accompany any federal, state and territory government proposal to introduce legislation that impinges on privacy.**[185]

Such a statement could include a Privacy Impact Assessment and an analysis of whether the government proposal is consistent with existing federal, state and territory laws relating to the regulation of privacy.

This may include consideration of privacy matters other than the protection of personal information. See Chapter 6 for further discussion of Privacy Impact Assessments for new legislation.

[183] Australian Government Office of Regulation Review, *A Guide to Regulation—Second Edition: December 1998* (1999), B3–B4.

[184] Ibid, B2–B3.

[185] Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

Excerpt 2

6. Powers of the Office of the Privacy Commissioner

Advice on proposed enactments

6.31 **The Commissioner is to examine a proposed enactment that would require or authorise acts or practices of an agency or organisation that might, in the absence of the enactment, be an interference with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals. The Commissioner is to ensure that any adverse effects of such proposed enactment on the privacy of individuals are minimised**.[38]

6.32 **A document prepared as the result of such examination is popularly known as a 'privacy impact statement' or 'privacy impact assessment'**. As is the case with most of the powers inherent in the functions of the Commissioner established by **the *Privacy Act***, the power to examine a proposed enactment and advise on it is relatively wide. It **does not require, however, that a Minister obtain a privacy impact assessment, or that any assessment that is obtained be acted on**.[39]

6.33 **It has been suggested that privacy impact assessments should be required for all proposed Commonwealth legislation, or all proposed Commonwealth legislation carrying a high risk of infringing privacy rights created by the *Privacy Act*.**[40]

If that suggestion were adopted, **the issue arises as to whether the task should be performed by the OPC, some other public officer (currently existing or not), or a private sector individual or organisation**.

A related question is whether all privacy impact assessments should be subject to the same requirements (including as to whom should complete the task).

6.34 **The OPC Review raised the possibility that private sector organisations that develop and implement 'large scale high privacy risk' technology should be encouraged to conduct privacy impact assessments**.[41] The OPC has recently released guidelines for agencies in this regard, and the same approach could be applied to organisations.[42] The OPC Review did not go further to discuss whether organisations planning large scale high privacy risk projects should be *required* to prepare, or obtain, a privacy impact assessment, or whether privacy impact assessments are desirable or should be required other than in relation to technology. However, **the Senate Committee privacy inquiry recommended that the *Privacy Act* 'be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information'**.[43]

> **Question 6–6:** Should the *Privacy Act* require a privacy impact assessment to be prepared for:
>
> (a) all proposed Commonwealth legislation;

(b) other proposed projects or developments of agencies; or

(c) other proposed projects or developments of organisations?

Question 6–7: If privacy impact assessments are required:

(a) who should be involved in preparing the assessments;

(b) who should be entitled to view the results of the assessments;

(c) who should bear the cost of the assessments; and

(d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

[37] *Privacy Act 1988* (Cth) s 27(1)(k).

[38] Ibid s 27(1)(b).

[39] Note however that the Australian Government Department of the Prime Minister and Cabinet, ***Legislation Handbook* (1999)**, [4.7(h)(vi)] **provides that, in relation to legislative matters going before Cabinet, it is expected that the relevant department undertake other consultations in preparing the submission, including 'with the Privacy Commission if the legislation has implications for the privacy of individuals'**.

[40] Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

[41] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 256. This possibility was also discussed in the following consultations: Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

[42] See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006).

[43] Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 5. It is not clear whether this relates to agencies and/or organisations. The OPC has defined 'project' to include any proposal, review, system, database, program, application, service or initiative that includes the handling of personal information: Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 3. The ALRC understands 'developments' to refer to new technological developments, such as biometrics.

Excerpt 3

6. Powers of the Office of the Privacy Commissioner
Further obligations on agencies and organisations

6.174 The OPC Review noted that a 'number of submissions put the view that at present, the *Privacy Act* does not provide sufficient powers to ensure that businesses are aware of their obligations to protect privacy, or know how to implement them in practice and carry through on implementation'.[264] Some **suggestions about further obligations on agencies and organisations made to the OPC Review, the Senate Committee privacy inquiry or the ALRC have included**:

- extending the Commissioner's audit powers to the private sector;
- introducing self-auditing and reporting requirements;
- requiring organisations to make available an approved internal dispute resolution process;[265]
- requiring organisations when collecting information to inform individuals of their ability to make a complaint about a privacy issue;[266]
- **requiring the preparation of privacy impact assessments in more situations**;[267]
- requiring mandatory reporting of privacy breaches.[268]

[264] Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (2005), 135.

[265] Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.24], [6.37].

[266] Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (2005), 160 and Rec 41. See also Ch 4.

[267] Ibid, 256; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 5; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

[268] See Question 4–35 and Question 11–3(d). See also N Miller, 'Data Leaks Under Review', *The Sydney Morning Herald* (Sydney), 8 August 2006, 27; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006 and M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006.

Excerpt 4

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation
Census and Statistics Act 1905 (Cth)

7.92 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).[173] The census is regarded as the most important source of statistical information in Australia. The information from the census is used to produce statistical data for use by governments, as well as academics, industry, businesses and private

individuals. The ALRC is interested in hearing whether personal information collected for the purposes of the *Census and Statistics Act* is adequately protected.

7.93 In the late 1970s, the ALRC conducted an inquiry into privacy issues and the census, culminating in the release in 1979 of *Privacy and the Census* (ALRC 12).[174] The report made a number of recommendations directed to the protection of personal information collected as part of the census.[175] A number of these recommendations have been implemented.[176]

7.94 Following the release of ALRC 12 the *Privacy Act* was enacted. The *Privacy Act* applies the IPPs to personal information collected as part of the census.[177] For example, personal information collected by the ABS for a census is likely to be regarded as collection for a lawful purpose directly related to a function or activity of the ABS and necessary and directly related to that purpose.[178] The *Census and Statistics Act* also contains a number of provisions, including secrecy provisions, directed to the protection of information collected as part of the census.[179] For example, s 19A provides that the Statistician or an ABS officer must not at any time during the period of 99 years from the day for a census divulge or be required to divulge information contained in a census form to an agency, a court or a tribunal.[180]

7.95 Before the 2001 Census, all name-identified information from past census was destroyed on completion of statistical processing. In 2000, the Australian Government introduced legislation that provided for the retention of census data.[181] This legislation was put in place for the 2001 Census on a trial basis. The *Census Information Legislation Amendment Act 2006* (Cth) amended the *Census and Statistics Act* to ensure that, subject to the household's consent, name-identified information collected in the 2006 Census and all subsequent census would be stored by the National Archives to be preserved for release for future research after a closed access period of 99 years.[182]

7.96 Another recent development is the Census Data Enhancement (CDE) project.[183] **The primary objective of the CDE project was to enhance the value of the census by combining it with future census and possibly other datasets held by the ABS. The central feature would have been the Statistical Longitudinal Census Dataset (SLCD) involving all respondents to the census**. A Discussion Paper on the project was released in April 2005[184] and a Privacy Impact Assessment (PIA) was prepared.[185] Although there was some support for the project, **a number of submissions and the PIA identified significant privacy-related concerns**.[186] In particular, the PIA noted that the proposal will create a data resource so rich and valuable for administrative uses that the privacy and secrecy framework under which the ABS operates may come under great and possible irresistible pressure, if not immediately, then at least in the medium to long term … Despite the rigour of the legislative protections, and the ABS track record both of procedural safeguards and of defence of the principle of confidentiality, there remains a residual privacy risk of future changes in legislation to allow administrative and other nonstatistical uses.[187]

7.97 On 18 August 2005, the ABS announced that it would not proceed with the SLCD as proposed and that the CDE proposal had been substantially modified.[188] **The SLCD will now be based on a 5% sample of the population**. It is the ABS's view that the reduction of the dataset to a 5% sample will make the dataset unsuitable for administrative and other non-statistical uses. Despite the modifications, the APF still have a number of concerns about the proposal, including that data collected in each census will now be retained and linked, will cover one million people, and may be used in conjunction with data from other sources.[189]

[173] Census and Statistics Act 1905 (Cth) s 8.

[174] Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).

[175] Ibid, x–xvi.

[176] See, eg, Census Information Legislation Amendment Act 2000 (Cth).

[177] The ABS is an 'agency' for the purposes of the *Privacy Act*: *Privacy Act 1988* (Cth) s 6. For a discussion of how the IPPs apply to the census see House of Representatives Legal and Constitutional Affairs Committee—Parliament of Australia, *Saving Our Census and Preserving Our History* (1998), Ch 4.

[178] *Privacy Act 1988* (Cth) s 14, IPP 1.1.

[179] *Census and Statistics Act 1905* (Cth) ss 7, 8A, 13, 19, 19A, and 19B. Further, the *Statistics Determination 1983* (Cth) made by the Minister under *Census and Statistics Act 1905* (Cth) s 13 provides for the disclosure, with the approval in writing of the Statistician, of specified classes of information.

[180] See House of Representatives Legal and Constitutional Affairs Committee—Parliament of Australia, *Saving Our Census and Preserving Our History* (1998), Rec 1. See also Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

[181] Census Information Legislation Amendment Act 2000 (Cth).

[182] Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

[183] Australian Bureau of Statistics, *Census of Population and Housing—Census Data Enhancement* <www.abs.gov.au> at 25 August 2006.

[184] Australian Bureau of Statistics, Enhancing the Population Census: Developing a Longitudinal View (2005).

[185] Pacific Privacy Consulting, Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics (2005).

[186] See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.113]–[5.116].

[187] Pacific Privacy Consulting, Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics (2005), 3.

[188] Australian Bureau of Statistics, 'ABS Develops a New View of Records Across Successive Censuses' (Press Release, 18 August 2005).

[189] Australian Privacy Foundation, *Privacy Concerns with the 2006 Census* (2006) <www.privacy.org.au/Campaigns/Census> at 24 August 2006.

Excerpt 5

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation Anti-Money Laundering and Counter-Terrorism Financing Bill 2006

7.105 On 13 July 2006, the Minister for Justice and Customs, Senator the Hon Chris Ellison, released for public consultation a revised exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) (AML/CTF Bill 2006) and draft Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF Rules).

7.106 The AML/CTF Bill 2006 is intended to enable individual businesses to manage money laundering and terrorism financing risks. The Bill sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person who provides 'designated services'.[199] A large number of 'designated services' are listed in the Bill including opening an account, making a loan, and supplying goods by way of hire purchase.[200]

7.107 The Bill requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer.[201] In addition, reporting entities must give the Australian Transaction Reports and Analysis Centre (AUSTRAC) reports about suspicious matters,[202] and must have and comply with an anti-money laundering and counter-terrorism financing program.[203] The Bill also imposes various record-keeping requirements on reporting entities.[204] For example, a reporting entity must make a record each time it provides a designated service and must retain the record for seven years.[205]

7.108 Part 11 of the Bill relates to secrecy and access. Except as permitted by the Bill, an AUSTRAC official, a customs officer or a police officer must not disclose information or documents obtained under the Bill.[206] Further, a reporting entity must not disclose that it has reported, or is required to report, information to AUSTRAC; or that it has formed a suspicion about a transaction or matter. The Part also provides that the Australian Taxation Office and certain other 'designated agencies' may access AUSTRAC information. The term 'designated agencies' is defined in cl 5 to include a large number of Australian Government agencies as well as some state and territory agencies. Designated agencies may access AUSTRAC information for the purposes of performing that agency's functions and exercising the agency's powers.[207] The Bill requires designated agencies, including state and territory agencies, to comply with the IPPs in respect of the accessed AUSTRAC information.[208]

7.109 The revised exposure draft AML/CTF Bill 2006 and draft AML/CTF Rules reflect consideration of over 120 submissions provided to the Attorney-General's Department following the release of the first exposure Bill on 16 December 2005,[209] and **the findings of the Senate Legal and Constitutional Legislation Committee inquiry into the exposure draft Bill**.[210] **The Committee concluded that an independent privacy impact assessment of the Bill should be conducted**. The Committee also recommended that the Bill should contain a statement that is reflective of the intention to allow federal, state and territory agencies to access and utilise AUSTRAC data for purposes that may not be related to anti-money laundering or counter-terrorism financing.[211] These recommendations have not been included in the latest revised exposure draft of the Bill.

7.110 Submissions in response to the revised exposure draft AML/CTF Bill 2006 continue to raise privacy issues. For example, the OPC and the APF have both observed that while Part 11 of the Bill imposes some privacy obligations on state and territory agencies accessing AUSTRAC information, not all states and territories have enacted privacy regimes. Therefore, it is unclear whether individuals will be able to make complaints and seek remedies if information has been dealt with inappropriately by these agencies.[212]

7.111 Submissions have also noted that the NPPs may not provide adequate protection of personal information collected and disclosed under the Bill. For example, reporting entities that are 'organisations' for the purposes of the *Privacy Act* will have to comply with the NPPs. However, the NPPs will generally not apply to reporting entities that are small businesses.[213] A proportion of the reporting entities that are collecting and sharing personal information for the purposes of the Bill therefore may not be subject to any privacy regulation.

7.112 Under Part 10 of the Bill a reporting entity must retain for seven years information contained in a suspicious matter report to AUSTRAC. However, the Bill prevents an individual from seeking access to that information under NPP 6. The OPC has therefore suggested that, as an individual is not able to check information that is held about his or her, and has no opportunity to provide clarifying details or correct errors, further limitations on the retention of information by reporting entities are warranted.[214] It has also been observed that cl 110 of the Bill makes it an offence to provide a designated service on an anonymous basis. This directly contradicts NPP 8 which provides that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[215]

7.113 The Attorney-General's Department is currently reviewing the submissions received during the second consultation period and is finalising the legislative package for introduction to Parliament later in 2006. The ALRC is interested in views on how the Bill interacts with the *Privacy Act* and whether the Bill adequately protects personal information.

[199] Revised Exposure Draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) cl 5.

[200] Ibid cl 6.

[201] Ibid pt 2.

[202] Ibid pt 3.

[203] An anti-money laundering and counter-terrorism financing program is a program that is designed to identify, mitigate and manage the risk a reporting entity may face when providing designated services in Australia that might involve or facilitate money laundering or financing of terrorism: Ibid cl 74.

[204] Ibid pt 10.

[205] Ibid cl 85.

[206] See, eg, Ibid cl 93.

[207] Ibid cl 99.

[208] Ibid cl 99(3).

[209] See Australian Government Attorney-General's Department, *Welcome to Anti-money Laundering Reform Online* <www.ag.gov.au> at 27 August 2006.

[210] Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005* (2006).

[211] Ibid, [4.72]–[4.76].

[212] See, eg, Australian Government Office of the Privacy Commissioner, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, 3; Australian Privacy Foundation, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, August 2006, 57.

[213] See, eg, Australian Government Office of the Privacy Commissioner, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, 3–4; Australian

Privacy Foundation, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, August 2006, 62; Chartered Secretaries Australia, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, August 2006.

[214] Australian Government Office of the Privacy Commissioner, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, 4.

[215] Ibid, 5.

Excerpt 6

11. Developing Technology

11.37 In 2006, **the Australian Government released part of a framework to assist agencies seeking to implement smart card technology**.[65] **The framework requires** agencies implementing smart card technologies to include data protection clauses in agreements with third parties about the supply of smart cards and related services, and **privacy impact assessments to be undertaken during the design of smart card systems**. It also requires agencies implementing smart card technologies to produce comprehensive privacy policy statements and to revise these statements 'whenever a third party agency adds additional functionality to an existing smartcard deployment'.[66]

[65] Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006).

[66] Ibid, [a.17].

Excerpt 7

11. Developing Technology

11.47 On 27 July 2006, the Privacy Commissioner announced the approval of the *Biometrics Institute Privacy Code*.[95] The preamble to the Code notes that 'Biometrics Institute members understand that only by adopting and promoting ethical practices, openness and transparency can these technologies gain widespread acceptance'.[96] The Code is binding on Biometrics Institute members who sign the Biometrics Institute Privacy Code Agreement to Comply.[97] To date, two organisations have agreed to be bound by the Code.[98]

11.48 The Code aims to: (i) facilitate the protection of personal information provided by, or held in relation to, biometric systems; (ii) facilitate the process of identity authentication in a manner consistent with the *Privacy Act* and the National Privacy Principles (NPPs); and (iii) promote biometrics as PETs.[99] It includes information privacy standards that are at least equivalent to the NPPs.[100] In addition, it requires organisations that have agreed to be bound by the Code to observe higher levels of privacy protection than those in the NPPs in certain circumstances. For example, the Code applies to acts and practices relating to employee records that are exempt from the operation of the *Privacy Act* if a biometric is included as part of the employee record, or has a function related to the collection and storage of, access to, or transmission of an employee record.[101]

11.49 **The [Biometrics] Code** also contains three new information privacy principles. Principle 11 (Protection) sets out the steps that Code subscribers must take to protect biometric information, including ensuring that biometric information is de-identified where practicable, only stored in encrypted form and is not held in a way that makes it easy to match to other personal information. Principle 12 (Control) requires enrolment in biometric systems to be voluntary, and prevents organisations from using biometric information for some secondary purposes without 'free and informed consent'. **Principle 13** (Accountability) requires individuals to be informed of the purposes for which a biometric system is being deployed. It also requires biometric systems to be audited and Code subscribers to adopt a holistic approach to privacy policy and procedures. In addition, it **mandates the use of privacy impact assessments as part of the planning and management process for biometrics implementation**.

[Note: virtually no organisations at all have subscribed to the Biometrics Code, and it does not even automatically apply to members of the organisation that sponsored it]

[95] K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

[96] Biometrics Institute, *Biometrics Institute Privacy Code* (2006), Preamble, [2].

[97] Ibid, [C.1], [C.2].

[98] Biometrics Institute, Biometrics Institute Privacy Code—Public Register (2006) <www.biometricsinstitute.org> at 4 September 2006.

[99] Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [B.1].

[100] K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

[101] Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [D.5].

II. New South Wales

N.S.W. is a State of about 800,000 square kilometers (20% larger than France). It has a population approaching 7 million, almost 75% of whom live in the Newcastle-Sydney-Wollongong conurbation.

Legislative and Policy Framework

Legislation

From 1975 until 1999, the NSW Privacy Committee operated as a research and complaints-handling body. Since 1999, there has been an Office of the New South Wales Privacy Commissioner (Privacy NSW).[32] The Commissioner on a part-time basis from 1999 until May 2003 was Chris Puplick. Since September 2003, John Dickie, sometime Chief Censor, has been Acting in the position, full-time since the end of 2004, but on rolling short-term contracts.

The primary legislation is the *Privacy and Personal Information Protection Act* (PPIPA).[33]

Relevant New South Wales laws include:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *Freedom of Information Act 1989*
- *State Records Act 1998*
- *Criminal Records Act 1991 (Spent Convictions)*
- *Listening Devices Act 1984*
- *Workplace Surveillance Act 2005*
- *Telecommunications (Interception and Access) (New South Wales) Act 1987*
- *Access to Neighbouring Land Act 2000, esp. s.16 and s.26.*
- *Crimes (Forensic Procedures) ACT 2000*[34]

PIA Guidance Material

There is currently no official PIA guidance material in NSW. The web-page for Government, which appears to have been in its present form since about 2004, refers to PIAs as follows:

"PIA involves a comprehensive analysis of the likely impacts of a project upon the privacy rights of individuals. It is a little ... like an environmental impact assessment done for a new development proposal. The assessment can ensure that any problems are identified – and resolved – at the design stage. PIA is not only about ensuring compliance with the relevant information privacy laws (such as the PPIP Act and the HRIP Act), but can also help to minimise the risk of reputational damage by identifying broader privacy concerns (such as bodily or territorial privacy impacts).

[32] The NSW Privacy website is at: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index.
[33] The Act may be found at: http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/.
[34] Listed on the Privacy Commissioner of Australia website at: http://www.privacy.gov.au/privacy_rights/laws/ and Australian Privacy Foundation website at: http://www.privacy.org.au/Resources/PLawsST.html#NSW.

"**Privacy NSW hopes to develop a guide to conducting PIAs in the near future**. Similar jurisdictions to NSW have or are currently developing their own guides; if you would like to find out more about these please contact Privacy NSW".[35]

The page offers a checklist of privacy issues that agencies may need to address. The hotlink is broken, but it can be found at:

https://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/privacyessentials_03_2005.pdf/$file/privacyessentials_03_2005.pdf

The following extract is taken from the Commission's June 2004 Submission to a Review of the Privacy and *Personal Information Protection Act 1998*. It cited Blair Stewart's papers, and referred to the literature and brief history in one of this author's papers (emphasis added).

> "Under the PPIP Act, public sector agencies are required to prepare and publish Privacy Management Plans in relation to their compliance with the Act. However Privacy Management Plans do not embrace matters outside the regulatory scope of the PPIP Act, nor do they relate to specific projects, and there is no requirement to update their plans as new initiatives are being considered. **Our success in getting agencies to measure privacy impacts before undertaking new practices or projects has mostly been limited to ensuring compliance with regulatory requirements.**
>
> "**By contrast, a Privacy Impact Assessment (PIA) is a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal. PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated**.
>
> "A well-conducted PIA can provide assistance not only in terms of compliance with relevant privacy law, but also guidance for measuring the privacy impact of projects and practices which are not governed by information privacy laws. PIAs would also heighten the awareness and importance of privacy generally, and will bolster efforts to make privacy consideration part of the 'mainstream' legal and policy landscape.
>
> "Privacy Impact Assessment has been mentioned in the privacy literature from the 1980s, and implemented in jurisdictions from the early 1990s. PIAs have often been promoted by Privacy Commissioners as a way of encouraging more self-reliance by agencies, in terms of building expertise in privacy assessment outside of just the Commissioner's office.
>
> "Privacy and data protection commissioners have a central role in respect of the protection of privacy. However, they invariably have small budgets and few staff. It is absurd to expect that Commissioners can assess all the various technological initiatives likely to impact upon citizens' privacy in the coming years. The responsibility must be shared.
>
> "**The objectives of a PIA** may be to:
>
> - **assess risks arising from a new technology** or the convergence of existing technologies (for instance, electronic road pricing, caller ID, smart cards);
> - **assess risks where a known privacy intrusive technology is to be used in new circumstances** (for instance, expanding data matching or drug testing, installation of video surveillance cameras in further public places);
> - **assess risks in a major endeavour or change in practice having significant privacy effects** (for instance, a proposal to merge major public registries into a "super registry", to adopt a national ID card, to relax controls on telephone tapping or to extend powers of search of premises or persons); and to develop strategies for minimising those risks.

[35] http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_forgovt.

> "**PIAs, if published, can also address reputational risk areas for government, and can assist other similar projects by providing a ready-made analysis of likely risk areas and possible solutions**.
>
> "In the last few years PIAs have become compulsory for large federal government projects in the United States and Canada, and they have also been undertaken voluntarily by agencies in Hong Kong and New Zealand. A recent example from New Zealand, published on the Privacy Commissioner's website, related to the State Services Commission's project on authentication for e-government purposes.
>
> "In 2002 **the New Zealand** Privacy Commissioner published a **Privacy Impact Assessment Handbook** which provides guidance to both public and private organisations about how to conduct PIAs. The Handbook **is an exemplar of guidance and leadership in the area of best privacy practice**.
>
> "We understand that both the Office of the Federal Privacy Commissioner and the Victorian Privacy Commissioner are currently working on their own PIA handbooks, as they each recognise the growing importance of PIA as a valuable assessment tool for governments when developing new legislative and technological projects and policies.
>
> "**We believe that PIAs are the best means by which government agencies can aim for best privacy practice as well as legislative compliance. It is our submission that ideally, a PIA would be a statutory requirement for any new Bill, regulation, or project significant enough to require Cabinet consideration**.
>
> "One possible model would be:
>
> - Privacy NSW to help set terms of reference for a PIA, including what external guidelines / standards to use
> - PIA to be conducted by an independent consultant, who reports to Privacy NSW as well as the client
> - final PIA report to be published" [36]

The Commission has been starved of resources since mid-2004, and there appears to have been no subsequent progress.

On the other hand, the following extracts from the Privacy Commission's February 2007 Submission to the Australian Law Reform Commission's Review of federal Privacy Law indicates that it continues to be supportive of the notion, at least at federal level:

> "**Privacy legislation should make it mandatory for all Commonwealth agencies and private organisations to provide and publish Privacy Impact Assessments (PIAs) for all new programs, policies and draft legislation which impacts on the handling of 'personal information'. The PIA provides for accountability and greater transparency in decision-making.**
>
> "If PIAs were mandatory in certain circumstances, **it would create a consistent framework for the early identification of actual or potential privacy risks during the design and/or redesign of legislation, programs and services**. For example, the early identification of privacy risks in major IT projects has the potential to prevent costs that may be incurred through rushed modifications if the risk is identified late in the development process. In addition, the requirement for PIAs would create more awareness of the importance of privacy and make privacy compliance a fixture in today's legal and policy landscape.
>
> "Formalisation of the role of the Privacy Commissioner in regard to consultation of this nature concerning initiatives that impact on information privacy would only serve to have

36

http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_ppipareview.pdf/$file/sub_ppipareview.pdf#target='_blank'.

a positive effect on privacy protection. A PIA can provide assistance with compliance as well as a barometer for measuring the privacy impact of projects and practices.

"**The Privacy Commissioner could provide a guideline or 'template' for PIAs**, as well as input into matters which the OPC feels should be addressed with a specific assessment for comprehensiveness of outcome. However, we envision that **either an external consultant or the Privacy Commissioner could undertake a PIA**, provided there are no conflicts of interest.

"**The financial cost for PIAs should be shouldered by the agency/organisation seeking to initiate the new/revised legislation, program or services**. This prerequisite would be on the same order or similar to the requirement of environmental impact statements prior to proposed undertakings in the mining or construction industries. **To ensure openness and accountability, copies of these assessments should be provided to the Privacy Commissioner and made available to the public**".[37]

Completion of PIAs

Privacy NSW is aware that a few agencies have conducted PIAs. Although mention has been made in various discussions of PIAs in the health and education spheres, no evidence was found.

If anything, the tendency is in the other direction: the Government has suspended a Health Privacy Principle in respect of a major pilot project in the health care arena, because the pilot would otherwise have been in breach of the Act.[38]

[37] at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_alrc2007.pdf.
[38] http://www.smh.com.au/news/national/no-privacy-guarantee-on-new-health-records/2006/04/04/1143916530284.html http://www.smh.com.au/news/national/reversal-of-privacy-promise/2006/02/24/1140670269206.html. See also http://www.privacy.org.au/Campaigns/E_Health_Record/HealthElink.html.

III. VICTORIA

Victoria is a State of about 230,000 square kilometres (about the same as the U.K.). It has a population of 5 million, 75% of whom live in the capital city.

Legislative and Policy Framework

Legislation

A conventional statute, the *Information Privacy Act 2000*, came into effect in late 2002.[39]

There is also a separate Health Records Act.[40]

The *Information Privacy Act* created the statutory post of Privacy Commissioner. The post is supported by the Office of the Victorian Privacy Commissioner (OVPC), or Privacy Victoria.[41]

Relevant Victoria laws include:

- *Charter of Human Rights and Responsibilities Act 2006 (which includes reference to privacy)*
- *Information Privacy Act 2000*
- *Health Records Act 2001*
- *Freedom of Information Act 1982*
- *Public Records Act 1973*
- *Surveillance Devices Act 1999*
- *Telecommunications (Interception) (State Provisions) Act 1988* [42]

PIA Guidelines

In August 2004, the Commissioner published a 'Privacy Impact Assessment Guide'.[43]

The Australian Privacy Foundation expressed reservations, including: "the document may be a guide for Privacy Law Compliance Audit, but not for Privacy Impact Assessment. In addition, the document makes repeated mentions of the IPPs and the Information Privacy Act, and does not refer to the many additional laws that establish privacy protections" [and] "most of the Guide is written as though the exercise was purely internal".[44]

The Commissioner has communicated the existence of the PIA Guidelines through its network of privacy officers in government agencies, conducted a training session, and mentioned the PIA Guidelines in various presentations.

---

[39] http://www.austlii.edu.au/au/legis/vic/consol%5fact/ipa2000231/index.html
[40] http://www.austlii.edu.au/au/legis/vic/consol%5fact/hra2001144/index.html
[41] http://www.privacy.vic.gov.au/
[42] Office of the Privacy Commissioner of Australia at: http://www.privacy.gov.au/privacy_rights/laws/#2 and Australian Privacy Foundation, http://www.privacy.org.au/Resources/PLawsST.html#Vic.
[43] At: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf.
[44] http://www.privacy.org.au/Papers/OFPC-PIA-0502.rtf.

It is understood that the Department of Justice used the Commissioner's Guide as a basis for a practical document suitable for practitioners in the Department's organisational sub-units.

A draft document, presumably of 2005-06, implies that the Victorian Government Identity Management Framework suggests that a PIA be undertaken as part of projects that involve identity authentication[45]; but no final document could be found.

The Victorian PIA Guidelines

The PIA Guide of August 2004 references prior work, particularly in New Zealand, Canada and Hong Kong, and at federal level in Australia.

Key features include the following:

- it is specifically addressed to government agencies;
- it uses Blair Stewart's description of a PIA as "a systematic process for identifying and addressing privacy issues";
- it is limited throughout to the scope of the Victorian Act, and in particular to compliance with the legal requirements expressed primarily in the Information Privacy Principles;
- agencies are subject to no obligations in relation to PIAs. The Guide states, however that "A PIA should be completed for any new project or system, or any significant revision or extension of an existing system, involving the collection and handling of personal information" (p. 3, emphasis added in this document);
- "Ideally, a PIA should be initiated at the early stages of project or system development and planning" (p. 3);
- "Often, a PIA will be useful more than once in the project's life" (p. 3);
- "the object of a PIA is not to 'sell' an idea that may have adverse privacy implications. The primary object of a PIA is to allow any adverse effect on privacy to be weighed properly against whatever benefits the project or system offers in the public interest" (p. 4);
- "A [PIA] can be performed by: "an individual from within the organisation; a team or section from within the organisation; a joint team or working group if more than one organisation is involved in a project; or an external body ... [but] it will still be important for the organisation to have overall responsibility for the PIA" (p. 9);
- "PIAs form part of the risk evaluation and management tasks for any substantial undertaking" (p. 11);
- although the document mentions "public consultation as part of a PIA" and "publishing a PIA once it is complete", it expresses neither requirements nor recommendations (p. 13);
- in the case of agencies exempted from the Act ,or business processes that may be the subject of exceptions within the Act, it appears to absolve the agency of any responsibility to conduct a PIA (p. 14).

45 http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/IDAInternalGuidelinesOverview/$File/IDA%20Internal%20Guidelines%20Overview.pdf

Review of the Guidelines

The Commissioner has stated her intention to review the Guidelines in the near future, with the expectation that key messages will be strengthened and clarified. Some of the elements of this may include:

- the agency's responsibility to perform PIAs where privacy impacts of a measure may be significant;
- the benefits of using specialist support, at least in relation to the framing and planning of the PIA, even if the assessment itself is undertaken by agency staff;
- the Commissioner's role in PIAs, which she sees as being as a stakeholder, as an advisor prior to the commencement of the assessment, and as a discussant and reviewer of the outcomes, but not as a formal 'approver' of PIA processes or reports;
- the benefits of involving the affected public, their representatives, and advocates for their interests. These include deeper understanding of the impacts, and ways of solving the problems;
- the benefits of publishing the existence of PIA processes;
- the benefits of publishing the resulting PIA report;
- appropriate ways to deal with the media in relation to PIAs, in order to avoid trivialisation and mis-reporting, but nonetheless achieve a suitable level of transparency.

Practical advice to practitioners on how to go about doing a PIA is important, because agencies have conveyed the message that without it they are reluctant to adopt the technique.

Completion of PIAs

Examples of PIAs Conducted

It is understood that a small number of PIAs have been performed in Victoria, including one on a pilot health smartcard scheme.

The only published document of the nature of a PIA that could be located was performed by the Department of Education & Training (DET). It related to an R&D initiative, undertaken jointly with Oracle, to produce a prototype student-centric information system known as Ultranet. One feature of the scheme is a unique student identifier intended for all Victorian students, at all levels.[46]

The document is limited to a Privacy Act Compliance check, and involved little or no consultation with affected parties. It is understood that the Department intends to conduct a full PIA, but has not yet done so even in respect of the identifier, far less in relation to the project as a whole.

The Commissioner is aware of many agencies claiming to have conducted PIAs, but only a small number have involved consultation with her Office. Many of those that have come to her notice have been quite limited in their scope, and agencies appear to have been reluctant to expose them.

[46] The document is an undated draft apparently of June 2006, at: http://www.eduweb.vic.gov.au/edulibrary/public/teachlearn/student/S@CPIAReport.doc.

The Commissioner is not aware of any PIA Reports having been published, and indeed is not aware of any public declarations by agencies of PIAs being conducted, or having been conducted.

External Consultation

The Guidelines mention public consultation as part of a PIA, but express neither requirements nor recommendations.

Public Availability

The Guidelines mention the publication of a PIA once it is complete, but express neither requirements nor recommendations

IV. QUEENSLAND

Queensland is a State of about 1.8 million sq.km. (Spain, France, Germany and Poland combined), ranging from lush coastal lands via rich agricultural country to semi-desert. It has a population of 4 million, of whom about 55% live in the Brisbane-Ipswich-Gold Coast conurbation.

Legislative and Policy Framework

Legislation

There is no privacy legislation, and no statutory privacy protection body in Queensland. A regulatory framework exists in the form of an unenforceable code expressed in two Government Standards – No. 42, plus No. 42A for health matters.[47] The Standards reflect the federal National Privacy Principles. They apply to almost all government agencies, but not to local government:

The Privacy Standard requires production of 'Privacy Plans', which detail how each agency has implemented the Principles.[48]

Relevant Queensland privacy laws include:

- *Freedom of Information Act 1992*
- *Public Records Act 2002*
- *Criminal Law (Rehabilitation of Offenders) Act 1986* (spent convictions)
- *Invasion of Privacy Act 1971*(listening devices, invasion of privacy of the home)
- *Whistleblowers Protection Act (1994)*
- *Police Powers and Responsibilities Act 2000* (Chapter 4 deals with Covert Evidence Gathering Powers) [49]:
- No state telecommunications interception power
- *Grosse v Purvis [2003] QDC 151 (16 June 2003)*
- *Private Employment Agents (Code of Conduct) Regulation 2005* (Provisions 14 and 15 deal with work seekers information and the need to ensure it is not disclosed or improperly used)

A small Privacy Unit within the Department of Justice and Attorney-General has some some responsibilities relating to privacy. The Department uses the label 'Queensland

[47] Current Information Standards, Guidelines and Reviews, IS42 and IS42A, Queensland Government at: http://www.governmentict.qld.gov.au/02_infostand/standards.htm.
[48] Futher explained at: http://www.privacy.qld.gov.au/plan.htm.
[49] From: http://www.privacy.gov.au/privacy_rights/laws/#3. This list and further notes are available at the Australian Privacy Foundation webpage at: http://www.privacy.org.au/Resources/PLawsST.html#Qld.

Privacy' for the web-page, but whereas in NSW and Victoria that form of title indicates a government agency, in this case it appears to be a slogan or brandname.[50]

Guidance Relating to PIAs

The Department of Justice and Attorney-General) has been conducting preliminary work and promising PIA guidance material since 2005.

Issue 2 of a newsletter called *Queensland Privacy (in focus)* in December 2005, stated that:

> "Privacy Impact Assessment (PIA) Annotated Questionnaire has been piloted in some Queensland Government agencies in relation to proposed programs and initiatives. Work continues on the questionnaire in relation to expanding use of the PIA process to assess proposed legislation or legislative amendments.
>
> "PIA guidelines will be available in February 2006 as a decision-making and privacy assessment tool complimentary [sic] to the PIA annotated questionnaire".[51]

Issue 3 in March 2006 stated that:

> "Privacy Impact Assessment (PIA) Annotated Questionnaire and Instructions—A 2-part PIA Annotated Questionnaire (1— Proposed programs, 2—Proposed legislation) and the complimentary [sic] completion instructions are in the final drafting stage and will be made available online shortly".[52]

Issue 6 in December 2006 stated that:

> "Privacy Impact Assessment (PIA) annotated questionnaire and instructions available online soon".[53]

At this stage, however, only the following guidance is provided:

> "What is a PIA?
>
> "**A Privacy Impact Assessment (PIA) is a due diligence exercise, allowing Queensland Government agencies (including relevant contractors, vendors, outsourcers and others) to identify and address potential privacy risks** that may occur during the course of their operations.
>
> "PIAs provide a thorough **description and analysis of a program, potential privacy risks** associated with the program, **and measures taken to minimise or eliminate such risks**. The PIA process may also be used to examine proposed legislation or legislative amendments.
>
> "When should Queensland government agencies conduct a PIA?
>
> "PIAs should be conducted whenever a program involving the collection, storage, use and/ or disclosure of personal information is proposed, or where existing programs may be substantially changed. PIAs should also be conducted where legislation (or a legislative amendment) affecting personal information is proposed.

[50] See http://www.privacy.qld.gov.au/ for the privacy guidance material provided by this agency and http://www.justice.qld.gov.au/dept/privacy.htm for information about the privacy scheme.
[51] At: http://www.privacy.qld.gov.au/publications/INfocus2.pdf.
[52] At: http://www.privacy.qld.gov.au/publications/INfocus3.pdf.
[53] at: http://www.privacy.qld.gov.au/publications/INfocus6.pdf.

> "It is not mandatory for Queensland government agencies to conduct PIAs, however **completed PIAs provide a high level of documented assurance to stakeholders (such as other Government agencies and members of the community)** that privacy issues relating to proposed programs, legislation or legislative amendments have been identified, considered and appropriately addressed.
>
> "PIA framework and agency checklist
>
> "Coming soon!
>
> "**A framework for PIAs is being developed** by the Department of Justice and Attorney-General. It will include agency checklists for proposed programs and legislation/ legislative amendments, as well as instructions for completing the checklists". [54]

Examples of PIAs Conducted

It is understood that a PIA was performed for the Department of Transport in relation to the proposed smartcard-based driver's licence, but it appears not to have been published.

No evidence was found of any other Queensland government agency having performed a PIA on any project or initiative.

[54] At: http://www.privacy.qld.gov.au/publications.htm#4.

V. WESTERN AUSTRALIA

Western Australia is a State of about 3 million sq.km. (and is the second-largest sub-national entity in the world, the size of 2/3rds of Russia west of the Urals, or close to Spain, France, Germany and the whole of Scandinavia combined). Most of it is desert or semi-desert. It has a population of about 2 million, about 75% of whom live in the capital city.

Legislative and Privacy Framework

Legislation

There is no privacy legislation in Western Australia. Relevant laws are at:

- *Freedom of Information Act 1992*
- *State Records Act 2000*
- *Spent Convictions Act 1988*
- *Surveillance Devices Act 1998*
- *Telecommunications (Interception) Western Australia Act 1996*[55]

Following the release of a Discussion Paper in 2003, the Attorney-General tabled an Information Privacy Bill in March 2007, but it has not progressed yet.[56]

The Bill contains a set of Information Privacy Principles and a separate set of Health Privacy Principles. It would expand the functions of the present Information Commissioner to that of a Privacy and Information Commissioner. Provision is made for a Deputy Commissioner, but there is no obligation to appoint one.

The Office of the Information Commissioner, which has existed since 1993, has been occupied on an Acting basis, on rolling contracts, since 2003. The Office has a total of 10 staff.[57]

The Bill would enable the post of Privacy and Information Commissioner to be held concurrently with that of Parliamentary Commissioner (Ombudsman). The Office of the Parliamentary Commissioner, which has existed since 1971.[58] The Bill contains no provisions relating to PIAs.

It does not appear that any agency is playing any interim role in relation to privacy protection.

[55] http://www.privacy.gov.au/privacy_rights/laws/#4 and http://www.privacy.org.au/Resources/PLawsST.html#WA.
[56] http://www.austlii.edu.au/au/legis/wa/bill/ipb2007241/
[57] Further information on the Office is available at: http://www.foi.wa.gov.au/.
[58] http://www.ombudsman.wa.gov.au/.

Completion of PIAs

Evidence was found of a single PIA Report. This was conducted in early 2007 in relation to a project to establish a Whole of Western Australian Government Number (WAGN) for public service employees[59].

As at 27 July 2007, the WAGN page contained the following text (emphasis added): [60]

> "**A PIA is an assessment tool that describes the personal information flows in an initiative** such as the WAGN, and analyses the possible impacts that those flows may have on the privacy of individuals. **The purpose of a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts**.
>
> "Some of the benefits of a PIA include the following:
>
> - gaining and maintaining **stakeholder acceptance** (including agencies and employees)
> - **early identification of privacy issues and risks** for the use of the WAGN by WA state government agencies
> - identifying privacy issues and risks in the disclosure or use of WAGN related information by WA state government agencies
> - **incorporating the management of identified issues and risk mitigation strategies into design** for development of the WAGN
>
> "The recommendations of the PIA will be used to inform policy, procedures and guidelines around the use of the WAGN. As **consultation with stakeholders is an important component of the PIA process**, the Office of e-Government is currently engaging with a number of WA state government agencies".

The PIA was undertaken following recommendations contained in a September 2005 consultancy report, at Appendix H (pp. 86-94).[61]

[59] http://www.egov.wa.gov.au/documents/FINALWAGNPIA.pdf
[60] "Western Australian Government Number Privacy Impact Assessment Consultation ," Office of e-Government, at: http://www.egov.wa.gov.au/index.cfm?event=consultation.
[61] "Identity and Access Management Framework," Department of the Premier and Cabinet, Western Australia Office of e-Government, September 15, 2005, http://www.egov.wa.gov.au/documents/idam_framework_final.swf.

VI. SOUTH AUSTRALIA

South Australia is a State of about 1 million sq.km. (France, Germany, Belgium and The Netherlands combined), most of it arid or semi-arid. It has a population of 1.5 million, over 70% of whom live in the capital city.

Legislative and Policy Framework

Legislation

Relevant South Australian laws include:

- *Freedom of Information Act 1991*
- *State Records Act 1997*
- *Listening and Surveillance Devices Act 1972*
- *Telecommunications (Interception) Act 1988*
- No spent convictions law, but see discussion paper (released 5 May 2004)[xvi][62]

There is no privacy legislation, and no statutory privacy protection body. A Privacy Committee of South Australia exists under proclamation of Government. It is run out of the State Records Office, and has no budget.[63]

A Handbook for Committee Members exists, which contains information on the role of the Committee, members' responsibilities and Committee processes and activities.[64]

One of the Committee's powers is to "exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit" (s.4 of the Proclamation establishing the Privacy Committee). It also handles complaints, advises Government and other bodies on privacy protection measures, and watches developments elsewhere.

A Cabinet Administrative Instruction 1/89 establishes a set of Information Privacy Principles, and includes the following Clauses:

4. The principal officer of each agency shall ensure that the following Principles are implemented, maintained and observed for and in respect of all personal information for which his or her agency is responsible.

6. An agency shall not do an act or engage in a practice that is in breach of or is a contravention of the Principles. [65]

Although, as a Cabinet Instruction, it is binding on all South Australian Public Sector agencies, it is unclear by what means and by whom it could be enforced.

The Department of Health Code of Fair Information Practice (July 2004) provides guidance in relation to the handling of personal information within "the Department,

[62] at: http://www.privacy.gov.au/privacy_rights/laws/#5 and http://www.privacy.org.au/Resources/PLawsST.html#SA.
[63] "Privacy Committee of South Australia, http://www.archives.sa.gov.au/privacy/committee.html.
[64] http://www.archives.sa.gov.au/files/privacy_privacy_committee_members_handbook.pdf.
[65] The Administrative Instruction is available at: http://www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf and: http://www.archives.sa.gov.au/privacy/principles.html.

funded services providers and others who have access to Departmental personal information".[66]

The Code is derived from the National Privacy Principles, and it appears that it embodies unspecified reductions in the protections declared in the Cabinet Instruction. As with the Cabinet Instruction itself, it is unclear whether, how and by whom it could be enforced, particularly in relation to organisations that are not State government agencies and individuals who are not State government employees.

The Department of Families and Communities has a Code of Fair Information Practice, which appears to be identical to the Health Code with the exception of the substitution of Departmental name.[67]

Guidance in Relation to PIAs

Apart from mention in an Annual Report of attendance by a representative of the Committee at a PIA Seminar in Wellington N.Z. in March 2006, the Committee's documents appear not to refer to privacy impact assessment.

The Executive Officer of the Committee advised that the South Australian Government does not have a centralised programme for Privacy Impact Assessment. However, "the Privacy Committee, supported by State Records, does use a rudimentary questionnaire for programmes that require Privacy Committee approval, exemption from the Information Privacy Principles, or require consideration of complex personal information handling issues. It is a working document that is adapted to suit the situation at hand. It may be formalised later, and adopt components from other jurisdictions' structured PIAs".

The Health Code makes reference to a PIA methodology tool. The Executive Officer of the Committee advised that the Department of Health has mandated PIAs for use in the early planning stages of projects involving personal information. A copy of the PIA Guidelines and Proforma were provided. The PIA Guidelines are broader than information privacy alone, but the PIA Proforma is limited to the Information Privacy Principles.

The Department of Families and Communities Code also makes reference to a PIA methodology tool, but it is unclear whether one has been developed, and if so whether any use has been made of it.

Examples of PIAs Conducted

It is to be presumed that PIAs have been performed within the Department of Health, but no information about them appears to be publicly available.

No evidence was found of any other S.A. government agency having performed a PIA on any project or initiative.

No copies of published PIA Reports were located.

---

[66] at: http://www.health.sa.gov.au/DesktopModules/SSSA_Documents/LinkClick.aspx?tabid=57&mid=403&table=SSSA_Documents&field=ItemID&id=45&link=H%3a%5cTemp%5cHealth-Code-July04.pdf and also available from: http://www.health.sa.gov.au (under Publications / Guidelines).

[67] at: http://www.familiesandcommunities.sa.gov.au/DesktopModules/SAHT_DNN2_Documents/DownloadFile.aspx?url_getfileid=65 and is available from: http://www.familiesandcommunities.sa.gov.au (under Publications / Policies).

VII. TASMANIA

Tasmania is an island State of about 90,000 sq.km. (the same as Portugal, and twice the size of Switzerland). It has a population of close to 0.5 million, about 40% of whom live in the capital city.

Legislative and Policy Framework

Legislation

Relevant Tasmanian laws include:

- *Personal Information Protection Act 2004*
- *Freedom of Information Act 1991*
- *Archives Act 1983*
- *Annulled Convictions Act 2003 (spent convictions)*
- *Listening Devices Act 1991*
- *Telecommunications (Interception) Tasmania Act 1999*[68]

The Personal Information Protection Act 2004 came into effect on 5 September 2005. It applies to the public and local government sectors and the University of Tasmania.[69]

The Act is a weakened form of the OECD model. It does not create a statutory office responsible for privacy matters, nor does it assign such responsibilities to any existing agency. A complaints-handling function is created, and assigned to the Ombudsman. (The practice in the State has been to consolidate all forms of review in the Ombudsman's Office, including FOI, police and health matters). The Ombudsman has no powers to enforce decisions.[70]

The only privacy-related information on the web-site appeared many months after the Ombudsman became responsible for privacy complaints.[71]

Privacy and personal information matters did not warrant mention in the Ombudsman's Annual Reports for 2004-05 or 2005-06.

Completion of PIAs

No evidence was found of any Tasmanian government agency having performed a PIA on any project or initiative.

[68] At: http://www.privacy.gov.au/privacy_rights/laws/#6 and http://www.privacy.org.au/Resources/PLawsST.html#Tas.
[69] At: http://www.austlii.edu.au/au/legis/tas/consol_act/pipa2004361/.
[70] At:http://www.ombudsman.tas.gov.au/.
[71] at: http://www.ombudsman.tas.gov.au/personal_information_protection.

VII. AUSTRALIAN CAPITAL TERRITORY

The Australian Capital Territory (A.C.T.) is a district which had a limited form of self-government imposed on it by the federal Parliament in the late 1980s. The city's population is about 300,000.

Legislative and Policy Framework

Legislation

Relevant laws include:

- *Human Rights Act 2004* (which includes a right to privacy*)*
- *Privacy Act 1988 (Cth)* [72]
- *Health Records (Privacy and Access) Act 1997*
- *Freedom of Information Act 1989*
- *Territory Records Act 2002 (*public records*)*
- *Spent Convictions Act 2000*
- *Listening Devices Act 1992*[73]

The A.C.T. is the only jurisdiction in Australia that has enacted a Bill of Rights – the Human Rights Act 2004. In s.12, the Act provides people with **a right to not have their privacy, family, home or correspondence interfered with unlawfully or arbitrarily.**[74]

The Act is administered by a Human Rights Commissioner with a small staff. There is nothing on the HRC's site to suggest that privacy is seen as a significant element of its responsibilities.[75]

A decade before the Human Rights Act was passed, the Territory chose to adopt the Commonwealth Privacy Act 1988. The authority for that is the Australian Capital Territory Government Service (Consequential Provisions) Act 1994 (which followed on from the 1988 Act that imposed self-government on the Territory), in particular s.23, Schedule 2 and Schedule 3.[76]

Among other things, this allocates to the federal Privacy Commissioner the responsibility to perform the functions of an A.C.T. Privacy Commissioner. The Office of the Federal Privacy Commissioner is located in Sydney, however. For some years there was a small office in Canberra, but that is no longer the case, and it appears that the responsibility may be worn lightly.

Within the A.C.T. Government, the primary responsibility for scrutiny of legislation for compliance with the Human Rights Act and the Privacy Act, and for advice on policy development, rests with the Department of Justice and Community Safety (JACS), and

[72] At: http://www.privacy.gov.au/privacy_rights/laws/#8.
[73] At http://www.privacy.gov.au/privacy_rights/laws/#8 and http://www.privacy.org.au/Resources/PLawsST.html#ACT.
[74] At: http://www.austlii.edu.au//au/legis/act/consol%5fact/hra2004148/.
[75] See: http://www.hrc.act.gov.au/.
[76] At: http://www.austlii.edu.au/au/legis/cth/consol_act/actgspa1994806/index.html.

in particular the Human Rights Unit. But other aspects of public law have to date absorbed the available resources.

PIA Guidance Material

No guidance appears to be provided to A.C.T. government agencies in relation to PIAs.

Completion of PIAs

No evidence was found of any A.C.T. government agency having performed a PIA on any project or initiative. In addition to the government handling a great deal of personal data relating to its residents generally, the Department of Corrective Services is preparing to impose continuous RFID-based tracking on prisoners in its new facility. It does not appear that a formal PIA has been undertaken into this initiative.

While no formal PIAs appear to be carried out, the Human Rights Unit advises that **new legislation is scrutinised against the Human Rights Act**, and this evaluation could reasonably be expected to extend privacy, including privacy of the person, personal behaviour and personal communications. On the other hand, this scrutiny appears to be largely internal dialogue within the A.C.T. public service, with limited public information and consultation.

IX. NORTHERN TERRITORY

The Northern Territory is a Territory with self-government powers, subject to occasional over-ride by the Commonwealth. It is about1.4 million square kilometers. (about the same as Portugal, Spain, France and Germany combined). It is mostly desert or semi-desert, and has a population of 200,000, about one-third indigenous. About 50% of the population lives in the capital city.

Policy and Legislation Framework

Legislation

Relevant Northern Territory relevant laws includes:[77]

- *Information Act 2002* (privacy, FOI and public records)
- *Criminal Records (Spent Convictions) Act 1992*
- *Surveillance Devices Act 2000*
- *Telecommunications (Interception) Northern Territory Act 2001*

A statute addressing both freedom of information and privacy was passed into law in 2002 and came into effect in mid-2003 as the Information Act (long title: An Act to provide for public access to information held by the public sector, to provide for the correction of personal information held by the public sector, to provide for the responsible collection and handling of personal information by the public sector, to promote appropriate records and archives management in the public sector, and for related purposes).[78] The Act created the statutory post of Information Commissioner.[79] It also provides for review after 5 years, and the review may extend to consideration of PIA matters.

Policy

No written guidance has yet been provided to agencies concerning PIAs. However, the Commissioner encourages agencies to discuss matters with the OIC, and some success has been achieved in this area.

In addition, in January 2007 mention of PIAs was made in the Commissioner's Submission to the Australian Law Reform Commission in relation to its review of federal privacy law. This is indicative of a general feeling among the four supervisory agencies that exist in Australian jurisdictions that the time has come for PIAs to be a mainstream activity, and for Commissioners to have powers that go beyond the provision of guidance (emphasis added).[80]

> "Presently the OPC [the Office of the federal Privacy Commissioner] provides a significant level of advice in relation to proposals that raise privacy issues. A requirement to obtain advice in relevant cases is set out in the Cabinet

[77] http://www.privacy.gov.au/privacy_rights/laws/#7 and http://www.privacy.org.au/Resources/PLawsST.html#NT.
[78] At: http://www.austlii.edu.au/au/legis/nt/consol_act/ia144/
[79] See Office of the Information Commissioner (OIC) websites at: http://www.privacy.nt.gov.au/ and http://www.nt.gov.au/justice/infocomm/privacy/index.shtml.
[80] See (pp. 25, 26) at http://www.nt.gov.au/justice/infocomm/docs/ntic_sub_on_dp31.pdf.

Handbook. However, there is no statutory requirement to consult the OIC about proposals.

"For agencies at least, it is worth considering whether that process should be formalised by inclusion of a requirement to consult the OPC in relation to any proposal that may raise privacy issues. The requirement could be general in nature or limited to legislative proposals.

"This would not necessarily require preparation of a privacy impact assessment for every proposal that raises privacy issues. In many cases, issues that arise might simply be dealt with by informal consultation with the OPC. The process could, however, be supplemented by **a power on the part of the OPC to direct that a privacy impact assessment be undertaken as part of the development process in an appropriate case**.

"Such a process would not preclude parliament or government from making legislation in the form that it sees fit. It would however, ensure that they are adequately informed in relation to potential privacy issues before deciding on whether to make the legislation..

"For existing legislation that impacts on privacy, consideration should also be given to requiring review, including consultation with the **OPC**, at regular intervals to ensure that any intrusions into the privacy of individuals are still warranted.

"**The OPC should have the following powers:**

- **direct that a privacy impact assessment be undertaken prior to implementation of the proposal;**
- **approve the terms of reference for the assessment (prepared by, and at the cost of, the proponent);**
- **review and comment on the assessment.**

"**All costs associated with the assessment should be met by the proponent.** There should be nothing to stop the OPC conducting an assessment if resources are available and the Commissioner considers it appropriate.

"**Any assessment conducted in relation to an agency proposal should be made public at an appropriate time.**

"Again, it should be stressed that the process would not preclude the parliament or the government from making laws in the manner it sees fit. It would however ensure that they are fully informed in relation to privacy issues.

Completion of PIAs

No evidence was found of any N.T. government agency having performed a PIA on any project or initiative.

However, the OIC has been involved in discussions about an initiative referred to as 'Territory Services'. This is considering a common shopfront as a way to reduce the number of government offices and consolidate citizen-facing resources. Because this has significant privacy implications, the Commissioner recommended that a PIA be performed, and provided the team developing the initiative with copies of the Australian and Victorian PIA Guidelines.

APPENDIX F

Privacy Impact Assessments
Jurisdictional Report for New Zealand

CONTENTS

Context

New Zealand is a nation of 4 million people on two islands in the South Pacific that are together about 30% larger than the island of Great Britain. It has an integrated national government with no provinces, states or territories.

Legislative and Policy Framework

Legislation

In 1991, the *Privacy Commissioner* Act 1991 established the office of Privacy Commissioner and created a set of legal requirements for data matching.

In 1993, the *Privacy Act 1993* superseded the 1991 law.[1]

Despite its title, the statute's scope is largely limited to information privacy matters, although some of the research, education and consultation functions refer to 'privacy' unqualified by 'information'.

With few exceptions the Act applies across the public and private sectors.The Privacy Commissioner has the power to issue Codes of Practice that become part of the law, and the Office may either respond to an initiative from elsewhere or initiate the Code themselves. Codes may increase or reduce the protection afforded by the Act. Six are in operation, but none specifically relate to PIAs.

Public Sector Privacy Policy and Guidance Material

In January 1999, the NZPC published a 'Guidance Note in Information Matching Privacy Impact Assessments'. This was restricted in its scope to matching programmes, which (as discussed below) are the subject of specific requirements under the Act. The current version of the document is dated 2006.

In 2002, the NZPC published a 'Privacy Impact Assessment Handbook'.[2]

The launch included a series of implementation seminars held in three major cities. The Handbook was also distributed to international delegates at the 2nd ASPAC Forum on Privacy and Data Protection, held in Auckland in 2002.

The Handbook acknowledges the authorship of Blair Stewart, prior and parallel work in Alberta, Ontario and British Columbia, and interactions with Hong Kong. It also references prior publications by Stewart (1996, 1999, 2001), David Flaherty (2000) and Nigel Waters (2001).

Key features of the Handbook are summarised in Appendix 1.

'Information Matching Privacy Impact Assessments' (IMPIA) have been a statutory requirement for each matching programme approved since 1996. Most of the 80 authorised matches, of which 46 are currently operational, are understood to have been the subject of an IMPIA.[3]

---

[1] Privacy Commissioner of New Zealand, *Privacy Act Summary,* at: http://www.privacy.org.nz/privacy-act/privacy-act-summary/ and a link and instructions for accessing the Act on the official legislation website at: http://www.privacy.org.nz/privacy-act/the-privacy-act/

[2] Privacy Commissioner of New Zealand, *Privacy Assessment Handbook, at http://www.privacy.org.nz/library/privacy-impact-assessment-handbook.*

[3] Privacy Commissioner of New Zealand, *Operating Matches*, at http://www.privacy.org.nz/data-matching/operating-matches

The New Zealand PIA Processes

History of the PIA in New Zealand

In 1996, the then Assistant Commissioner Blair Stewart published one of the earliest papers on PIAs, in the Australian journal *Privacy Law & Policy Reporter*.[4]

As early as 1996-97, the then Commissioner, Bruce Slane, adopted a policy of encouraging PIAs in particular circumstances. During this period, tensions appear to have arisen between the Commissioner and the Department of Transport in relation to a project to establish a new driver licensing scheme and card. Recognising that the scheme would have substantial privacy impacts, a Cabinet Instruction was issued requiring the Department to perform a PIA.

As the Office moved towards establishing guidance for the conduct of PIAs over the following years, Stewart published a series of further papers, including a hard-copy collection of 'Approaches, Issues And Examples' in 2001. NZ also hosted an international symposium on PIAs in 2003.

During a presentation in Hong Kong in 2001, Stewart defined a PIA as "assessment of any actual or potential effects that a proposal may have on privacy and the ways in which any adverse effects can be mitigated". He clearly distinguished it from privacy compliance audit and legal opinion.[5]

The Tools

Appendix 1 provides a summary of the PIA Handbook that was published in 2002. Key features include:

- a broad definition including a clear distinction from compliance audit, and by reference to "the expectations of the general public, customers, clients or employees" rather than only to privacy law;
- use as 'an early warning system', "incorporated into the early phases of the project and system development", "as part of a wider business privacy strategy", and as "an integral part of the planning process";
- allocation of responsibility for a PIA "to the proponent of the proposal";
- broad applicability to "to any proposal that could intrude on reasonable expectations of privacy";
- applicable to "any public or private sector agency that handles personal information, particularly medium to large businesses and government departments";
- suggestion that there are "distinct advantages in outsourcing the preparation of a privacy impact report to lend impartiality to the process";
- conception of the PIA Report as "an evolving document which will become more detailed over time";
- suggestion that a "preliminary privacy analysis" be undertaken, followed by emphasis on the Terms of reference, description of the project and information flows, and relationship to the information life-cycle; and
- preference for "openness about the findings".

[4] Stewart, B. (1996a). 'Privacy impact assessments', *Privacy Law & Policy Reporter*, 3, 4 (July) 61-64, at http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/39.html

[5] Blair Stewart, Assistant Commissioner, Office of the Privacy Commissioner, New Zealand, *PIA: Some Approaches, Issues and Examples*, at http://www.pcpd.org.hk/misc/stewart/sld001.htm.

Completion of PIAs

By Whom, When and under what circumstances?

With a possible exception discussed immediately below, neither agencies nor corporations are under any legal obligation to conduct PIAs, under any circumstances. It is merely a recommendation by the Commissioner: "I commend New Zealand organisations to employ privacy impact assessment for significant new initiatives involving the handling of personal information".[6]

A possible exception arises in the case of Information Matching programmes. The Commissioner is required under s.13(1)(f) of the Act to examine legislation that authorises data flows between agencies, with particular emphasis placed on flows for the purpose of data matching programmes. These are subject to a set of principles expressed in s.98 of the Act. The Commissioner provides a Guidance Note on 'Information Matching Privacy Impact Assessments' (IMPIA).[7]

Generally, however, there is very little to cause organisations to perform PIAs at all, let alone professionally, other than the risk of a media or public backlash.

Two PIAs have been conducted in the context of the eGovernment programme managed by the State Services Commission (SSC), in particular in the context of identifiers, identity authentication, and a national identification scheme.[8]

Other examples of PIAs understood to have been conducted by New Zealand agencies, with links to the PIA Reports where available, include:

- Land Transport Safety Authority (LTSA), re driver's licences (1997)
- New Zealand Health Information Service, re a Mental Health Information Project (February 1999);[9]
- Ministry of Education, re a National Student Index Number (December 2000);[10]
- Ministry of Health, re public health;[11]
- a Maori Registration Service database;[12]
- Statistics NZ, re an Injury Statistics Project Pilot (May 2004);[13] and

[6] PIA Handbook, Foreword by the Privacy Commissioner, at http://www.privacy.org.nz/library/privacy-impact-assessment-handbook.

[7] The current version, dated 2006 is at: http://www.privacy.org.nz/library/guidance-note-for-departments-seeking-legislative-provision-for-information-matching, together with a document titled 'Views On The Information Matching Guideline', at http://www.privacy.org.nz/filestore/docfiles/82836507.doc.

[8] generally at: http://plone.e.govt.nz/services/authentication/policywork/privacy.html and specifically:

- re a proposed all-of-government identity authentication scheme (March 2003), at http://www.e.govt.nz/services/authentication/library/docs/authent-pia-200312/authent-pia-200312.pdf with an update (December 2004), at:http://www.e.govt.nz/services/authentication/library/docs/pia-200404/pia-200404.pdf; [link does not work]
- re a Government Logon Service (July 2005), at http://www.e.govt.nz/services/authentication/library/docs/gls-pia/gls-pia-2005.pdf

[9] at http://www.nzhis.govt.nz/documentation/mhinc/ak983340.doc.

[10] At: http://www.minedu.govt.nz/web/downloadable/dl5724_v1/download-final-formatted-pia-january-2001.doc.

[11] mentioned in the Commissioner's 2003 Annual Report (p. 50)..

[12] mentioned in the Commissioner's 2003 Annual Report (p. 50).

- Ministry of Social Development (MSD), re Linked Employer Employee Data (LEED, July 2007).[14]

The Commissioner's Office was not aware of any PIAs having been conducted in the private sector. The only mention of a private sector PIA that was located related to a 'Regional Diagnostic Laboratory Data Repository'.[15]

Who participates?

The Assistant Commissioner observed that there were only a limited number of people with the expertise to conduct PIAs or to advise on their planning and conduct. He sees it as being highly desirable that an external specialist be engaged in a PIA, in order to provide not only expertise, but also independence and credibility. A fully-independent externally-conducted PIA may be far preferable to one conducted by an internal staff-member with limited expertise and limited seniority. However the best balance, and the best outcomes for the organisation and the privacy interest alike, may be achieved by having the process managed by internal staff with sufficient expertise, seniority and independence, supplemented by external consultancy support.

External Consultation

In relation to the need for consultation to be a feature of an effective PIA, the Assistant Commissioner acknowledged the lack of any guidance in the Handbook. When the Handbook was being drafted in 2000-02, concern was felt about the need for those involved in a PIA process to have sufficient expertise, and the likelihood that members of the public would not be well-equipped to participate. Some acknowledgement of the public's interest in the proceedings is appropriate, however, at the very least in relation to applications of new technologies.

Review/Approval of PIAs

Internal Review

The Handbook appears to be silent on the question of internal review and sign-off, leaving the organisation to apply its own governance norms.

Central Agency Review

The Privacy Commissioner has no formal role, although the Handbook suggests that "The Privacy Commissioner can add value to the process by reviewing a privacy impact report". In practice, however, it appears that few are submitted.

Oversight Office Review and Acceptance

There is no requirement for copies of PIA Reports to be submitted to the Commissioner, but it is understood that the Office receives about 2 or 3 each year, of varying quality.

The appropriate role of the regulator is a continuing issue. The focus remains on benefits to the sponsoring organisation. The Commissioner may be consulted or not, and may be given a copy or not. If the Commissioner were to take up, or to have imposed upon it, any review function, then both resources and expertise would be

[13] at: http://www.stats.govt.nz/NR/rdonlyres/1AD12FED-E5D2-4AA1-AAA2-219F8C837940/0/PilotPrivacyImpactAssessment.pdf
[14] at: http://www.stats.govt.nz/NR/rdonlyres/AF33C141-395F-4165-B564-98EF6DC6B7E0/0/LEEDMSD.pdf
[15] at: http://hcro.enigma.co.nz/website/index.cfm?fuseaction=articledisplay&FeatureID=040904.

required. Crucially, the Commissioner lacks the power to do anything in the event that a review resulted in negative findings.

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

Despite Principle 12 stating that "Data integration must be conducted openly", there is no evidence of any Reports being publicly available, or even of any having been performed, and it is unclear what, if any, difference the policy statement has made.

These might together be regarded as imposing an obligation on agencies that are proposing to conduct an information matching scheme to conduct a PIA. The Commissioner is required under s.105 of the *Privacy Act* to report annually on each authorised programme carried out in that year. In the Annual Report for 2006, for example, the report, on about 40 active programmes, occupies pp. 31-93.[16]

But there appear to be no published IMPIA Reports, and it is unclear to what extent the agencies perform a PIA, and to what extent the work is performed instead by the Commissioner. The 2006 Report does, however, make mention on p. 46 of one IMPIA performed by the Ministry of Social Development in August 2005, relating to a match between its records and those of the accident compensation agency.

The operations of Statistics NZ are exempt from the use and disclosure provisions of the Privacy Act by virtue of Principles 10(f)(ii) and 11(h)(ii). The agency is undertaking a 'Data Integration' Programme, which draws identified personal data from other agencies, consolidates it, and draws on it to produce statistics. In recognition of the extraordinary nature of such activities being exempt from data protection law, Statistics NZ has sanctioned, since at least February 2006, that "a data integration business case must include a privacy impact assessment."[17]

It does not appear that any IMPIAs for Information Matching programmes have been published. Although the Commissioner compiles a Report on each programme, only 5 are available on the Commissioner's site, and the IMPIAs in question are not attached. Even these few evidence concern about at least some of the programmes and about the quality of the IMPIAs submitted.[18]

Apart from reports relating to Information Matching PIAs, there has been almost no mention of PIAs in the Commissioner's Annual Reports since the launch of the Handbook in 2002 (pp. 50-51).

Other PIA Tools and Processes in New Zealand

Apart from the IMPIA and PIA guidance documents, there do not appear to be any other documents of significance.

PIA Template and Process Review and Revision

[16] at: http://www.privacy.org.nz/filestore/docfiles/29398162.pdf.
[17] Data Integration Principle 3(c)), at: http://www.stats.govt.nz/about-us/policies-and-guidelines/data-integration-policy/default.htm.
[18] at: http://www.privacy.org.nz/data-matching/s-13-1-f-reports.

No formal review of the PIA Handbook has been conducted. The Guidance Note on IMPIAs, on the other hand, has been revised, and may be further revised in the near future.

Review of PIA Policy/Legislation

In relation to the possibility of using the Code power to specify the need for a PIA to be performed, the Assistant Commissioner indicated the appropriateness of the longstanding and deliberate policy of encouraging and enabling the conduct of PIAs by organisations that sponsor projects, and of leaving questions about the mandation of PIAs to the Government and the Parliament. Risks are perceived in generic mandation, although for some classes of project it may be entirely appropriate (e.g. data matching, databank construction by NZ Statistics, and consolidated health records).

Further refinements to the Guidance Note re IMPIAs is in progress. Long-awaited amendments to the Privacy Act may find their way into the Parliament during 2008, and these could include a statutory requirement for something similar to the 'program protocol' stipulated by the Australian Parallel Data Matching legislation.

Lessons Learned

Utility of PIAs in New Zealand

Although IMPIAs have been a requirement since 1996, the outcomes are not transparent, and hence it is not not entirely clear how effective that form of assessment really is. PIAs more generally do not appear to be undertaken in respect of many projects, and there is evidence of some public dissatisfaction with the situation.

Room for Improvement

The Privacy Commissioner recommended changes to the Act some years ago, and these may find their way into Parliament in 2008. These could include more substantive requirements in relation to IMPIAs.

Oversight Body

The Privacy Commissioner has a formal role only in relation to the limited IMPIA process. In relation to PIAs more generally, its powers are limited, and it can do little more than provide advice in the form of the Handbook, and encourage agencies and corporations to perform PIAs in appropriate circumstances.

Central Agency

It does not appear that any central agency plays any significant role in relation to PIAs.

Practitioners and the Public

Serious dissatisfaction has been expressed by a member of the public in relation to the ignoring by the Land Transport Safety Authority (LTSA) of the outcomes of the PIA relating to the driver licensing scheme in 1995-98:[19]

This was the subject of litigation by the complainant in the High Court.[20] The Commissioner was not a party to the proceedings. It is understood that lack of public

[19] "How the Land Transport Safety Authority Deceived and Defrauded the New Zealand Public, Parliament and the Privacy Commissioner," at: http://www.celticnz.co.nz/transport/Time_Line.htm.
[20] (McInnes v Minister of Transport, [2000] BCL 653, matter CP 240/99).

consultation was part of the argument underlying the alleged illegality of the scheme, and that the PIA was discussed in the Judgment; but no copy could be located.

No practitioners were interviewed during the course of the Study.

Research

This report reflects research variously conducted and updated during July 2007, including an interview with the New Zealand Privacy Commissioner's delegate, Blair Stewart, Assistant Privacy Commissioner (Policy).

Appendix 1: Key features of the PIA Handbook

1. The PIA process is **clearly distinguished from "privacy compliance audits**, privacy seals and associated self-regulatory initiatives and privacy enhancing technologies" (p. 3); and

   "Privacy compliance audits are carried out on existing systems to ensure their conformity with internal rules and external requirements in relation to privacy and data protection. By contrast, PIA focuses on understanding a proposed system (or the effects of proposed change to an existing system)" (p. 9).

2. Impact assessment generally is "the identification of future consequence of a current or proposed action" (p. 9); and

   PIA is **defined as** "a systematic process for evaluating a proposal in terms of its impact upon privacy" (p. 5).

3. The **benefits of a PIA** are that it "helps an agency to (p. 5):

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

   and (p. 6):

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

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

   and (p. 13):

   - "to inform decision-makers";
   - "to assuage alarmist fears";
   - "to alert the complacent to potential pitfalls";
   - "to ensure that a business is the first to find out about privacy pitfalls in its project, rather than learning of them from critics or competitors";
   - " to save money and protect reputation";
   - "**to bring privacy responsibility clearly back to the proponent of a proposal**";
   - "to encourage cost-effective solutions since it is cheaper to do things at the design phase to meet privacy concerns than attempt to retrofit after a system is operational";

   and (p. 29):

   - "building trust in electronic service delivery and maintaining competitive advantage";

- "a pro-active approach to privacy risk management [to avoid] litigation risk [and provide] tangible proof of compliance with privacy policies and commitment to data protection principles [as part of a] strategy for managing privacy risk";
- "the human factor, [by providing] clear leadership on privacy issues, ... championing a culture that is respectful of customers and citizens and implements effective privacy policies".

Q4) *What factors are seen as determining which projects need PIAs?*

4. PIA "**applies to any proposal that could intrude on reasonable expectations of privacy** or the rights enshrined in the Act" (p. 9); and

   "A PIA will sometimes go beyond just a 'system' being assessed to consider critical 'downstream' effects on people who are affected in some way by the proposal" (p. 9).

5. More specifically, **project characteristics that indicate the need for a PIA** include (p. 15):

   - "projects [that] are of such a scale or nature that the need for PIA is glaring. For example, a data-warehouse holding personal information on nearly all people in New Zealand";
   - " the application of cutting edge technology to an aspect of data processing where the effects are not widely understood or trusted by the public ...";
   - "[where] the surveillance capacity or intrusiveness may be of such a nature as to make the merits of a PIA seem obvious";
   - "virtually any project which will amass otherwise confidential information into accessible databases";
   - "merging internal business databases to enable new forms of client profiling";
   - "centralising a multi-national company's employee records";
   - "changing the way information is collected in customer interface systems ... ";
   - "[application of] a new technology or the convergence of existing technologies ...";
   - "where a known privacy-intrusive technology is to be used in new circumstances ...";
   - in a major endeavour or change in practice with significant privacy effects ...".

6. PIA "should be **useful to any public or private sector agency** that handles personal information, particularly medium to large businesses and government departments" (pp. 5, 13); and

   "PIA is a technique for any business or public body that is serious about the need to maintain customer trust and confidence" (p. 6); and

   PIA "can be used with a public policy initiative or a corporate project" (p. 9).

Q5) *What are the rules, norms or expectations about who should conduct the PIA?*

7. "There are **distinct advantages in outsourcing the preparation of a privacy impact report to lend impartiality to the process**. That may be critical in influencing consumer or public opinion. Nonetheless, it is feasible to undertake PIA in-house, using the skills and experience of the project team and the wider organisation" (p. 5);

   with detailed advice on pp. 13-14), including:

   "the assessor will work closely alongside the project team to fully understand the business, the project, the risks and the appropriate responses. Where the PIA is solely undertaken internally, thought should given to incorporating some external or independent oversight. One possibility is to use a privacy or data protection consultant to carry out such a check" (p. 14).

8. "as **part of a wider business privacy strategy**, a business may adopt a PIA policy. ... An organisation which intends to use assessment as an ongoing privacy management tool should establish a process for determining when a privacy impact report is required. ... It would also be feasible to prepare internal PIA templates or questionnaires tailored to the nature of the business and its internal policies" (p. 15).

9. "To be effective, PIA needs to be **an integral part of the project planning process** rather than an afterthought" (p. 9); and

   "An understanding of the kinds of questions that will arise in the context of PIA, as well as a sense of where risk may lie, should therefore be **incorporated into the early phases of the project and system development**. Ideally, full and detailed consideration of privacy issues should precede system design" (p. 17).

10. "However, sometimes it may only be possible to complete a PIA at later stages in the system development and acquisition phase. If so, the privacy impact report can be **an evolving document which will become more detailed over time**. ... Responses can be refined in revised versions of the privacy impact report (p. 17).

11. Guidance is followed in relation to **the PIA process**, as follows (p. 5):

    - **Preliminary privacy analysis** - is a PIA needed for this project?

      "At this point, an attempt should be made to briefly document key features of the project and issues which have been identified without detailed study. Preliminary privacy analysis can assist by:

    - informing the decision whether to prepare a privacy impact report;
    - defining resource requirements (such as the skills that might be needed by an assessor, whether the task is small or large);
    - suggesting terms of reference for the assessment;
    - providing a tool for initiating consultation with the Privacy Commissioner" (p. 17);
    - **Terms of reference** - setting the task for the assessment (p. 19);
    - **Describing the project and information flows** - accurately understanding, and clearly describing, the processes is essential before analysing the privacy risks (p. 22);
    - **Privacy analysis** - examining all aspects of the proposed system from obtaining to destruction of data (pp. 22-23), including:

      "The privacy analysis will **follow the information 'life cycle'** ... [and] works through issues of information collection and obtaining, then use, disclosure and retention of personal information, with a further section on risk assessment. ... It will highlight how the project changes any previous information handling practice and how this may affect individuals" (p. 22);

    - **Privacy risk assessment** - identify the risks and judge their nature and seriousness (pp. 24-25). Risks include:
    - "failing to comply with either the letter or the spirit of the Act, or fair information practices generally ...;
    - stimulating public outcry ...;
    - loss of credibility or public confidence ...;
    - underestimating privacy requirements with the result that systems need to be redesigned or retro-fitted at considerable expense".

    "An important consideration is **the expectations of the general public, customers, clients or employees**. Proposals may be subject to public criticism even where the

requirements of the Act have been met. If people perceive their privacy is seriously at risk, they are unlikely to be satisfied by a company which justifies its actions merely by pointing out that technically it has not breached the law.

"One task of the PIA is to sort out which risks are serious and which are trivial. The privacy impact report should identify the avoidable risks ...";

- **Privacy enhancing responses** - security safeguards, privacy enhancing technologies and other management and technological solutions (pp. 24-26), including:

"The privacy impact report should suggest **cost-effective measures to reduce [the risks] to an appropriate level**. ... Suitable responses can range from doing nothing, through to abandoning the project altogether ... Examining privacy enhancing responses to the identified risks does not simply involve a recitation of encryption levels, access controls and other security features. It should also address the information and management needs of the project. One significant question is often not asked at all: does the business need personal information about identifiable people to fulfil its purposes? There are now a range of technologies available which allow for financial transactions to be completed electronically on an anonymous basis (sometimes referred to as **Privacy Enhancing Technologies or PETs**)";

- **Implementation, and post-implementation review** (confusingly referred to in the Handbook as 'Compliance mechanisms') - ensure that responses are effective in operation and trigger action if change occurs or if the measures implemented prove ineffective (pp. 26-27).

12. Substantial guidance is provided in relation to **the PIA Report** (p. 23-29).

    Q8) *Is there an approval process for the PIA Report? If so, it is the process external and/or internal to the organisation?*

13. "The Privacy Commissioner can add value to the process by **reviewing a privacy impact report**, rather than having to investigate the practices of the business itself. This is cost effective for the Commissioner and less intrusive for a business" (p. 13); and

    "the Privacy Commissioner will be willing to receive a PIA for information and will have staff offer some feedback and constructive suggestions" (p. 14).

    Q7) *What circulation, publication or submission rules, norms or expectations exist?*

14. "Usually, there is merit in making completed privacy impact reports publicly available and organisations should consider posting the privacy impact report or a summary on their website. **Openness about the findings** can contribute to the maintenance of public trust and confidence in the organisation and can ensure that its fair practices and policies in relation to the handling of personal information are freely available" (p. 19).

15. "**The [organisation] that will ultimately use the proposed system [may] not itself undertake or commission the PIA**. For instance, a software development company might commission an assessment of a new business computer program which will be made available commercially for others to use. In other cases a government body, an industry group, or an association of several organisations might commission a PIA for a project that may affect a number of businesses (such as a credit reporting system to be used by credit providers or a public health database into which medical practitioners might provide data). In these cases the PIA will contribute to solutions from which many businesses may benefit and to the trust which each needs in order to confidently share data. If the planned projects are very similar, government departments, or affiliated businesses, should consider undertaking a generic or overarching PIA to avoid unnecessary duplication of effort" (p. 14)

16. "Certain projects will have **significant privacy implications in more than one jurisdiction**. Indeed, some initiatives will have truly global implications. In such cases, comment might be invited from the privacy commissioners of several countries before finalising the privacy impact report. A significant objective of a PIA in such projects may

be to ensure that the project meets or exceeds the data protection and information privacy requirements in all the relevant countries and achieves a level of trust amongst consumers and regulators" (p. 14).

APPENDIX G

Jurisdictional Report for Hong Kong

CONTENTS

Context

Hong Kong Special Administrative Region (HKSAR) is a small region of the People's Republic of China which continues to operate with a high degree of autonomy.

Although the legal system largely reflects the century spent as a U.K. colony, the cultural context is very different. For example, it is understood that the first Privacy Commissioner needed to develop a Chinese character-pair to enable the depiction of 'privacy' to non-English-speaking citizens.

This report reflects research variously conducted and updated during July 2007, including interactions with the Hong Kong Privacy Commissioner's delegate, Allen Ting, Acting Chief Privacy Compliance Officer.

Legislative and Policy Framework

Legislation

The Hong Kong Personal Data (Privacy) Ordinance (PDPO) has been in force since 1996.[1] Among other things, the Ordinance created the Office of the Privacy Commissioner for Personal Data (PCPD):[2]

The Ordinance does not mention PIAs. However, under s.8(1)(d), the Commissioner has a duty to examine proposed legislation that he considers may affect data privacy and report the results of his examination to the agency concerned.

There are no circumstances in which PIAs are required. The Privacy Commissioner may make suggestions under s.8(1)(c). Successive Commissioners have indicated the need for, and benefits of, conducting PIAs, and appear to have had success on at least one occasion in convincing an agency to conduct a PIA.

PIA Guidance Material

The Commissioner has not issued any publications on PIAs. The text in Appendix 1, extracted from a 2001 document dealing specifically with E-Business, appears to be the only guidance currently provided in the jurisdiction.

The Commissioner recommends that a PIA should be undertaken in any of the following circumstances:

- introducing new public policy initiatives that involve significant collection, processing and use of personal data;
- implementing a technological proposal with personal data involved that impacts upon a wide population; and
- where a major endeavour to change existing business practices entails significant increases in the scope of collection, use and sharing of personal data.

In his guidance material, the Commissioner states that "PIA is a process that may be applied to a wide range of E-Business proposals that may be intrusive in terms of

[1] Chapter 486, Personal Data (Privacy) Ordinance, at: http://www.pcpd.org.hk/english/ordinance/ordfull.html.

[2] See website of the Office of the Privacy Commissioner for Personal Data for Hong Kong at: http://www.pcpd.org.hk/.

reasonable expectations of privacy, or the privacy rights enshrined in the Ordinance. It has equal validity applied to a public policy initiative e.g. electronic road pricing, as it has to a corporate initiative e.g. online customer profiling for prospecting purposes."[3]

NZ Deputy Commissioner Blair Stewart has presented in Hong Kong on several occasions, and some of the wording in Appendix 1 appears to reflect his contributions. The Commissioner notes that many public bodies in other jurisdictions have issued materials guiding the conduct of PIAs, including the Privacy Commissioners of Australia and New Zealand.

The Hong Kong PIA

History and Development of the Hong Kong PIA

In early-to-mid 2000, it appears that the then Privacy Commissioner, Stephen Lau, advised the Immigration Department to conduct a PIA in respect of the planned replacement of the HKSAR ID Card.

In November, 2000, in the Newsletter of the Office of the Privacy Commissioner for Personal Data, Issue No.5, the then Privacy Commissioner wrote:

> "Privacy Impact Assessment (PIA) should be conducted as an integral part of the planning and development of [the new HKSAR ID Card]. PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated".[4]

In December 2000, in a speech on 'Personal Data Privacy Issues of E-Medicine', the then Privacy Commissioner said:

> "A Privacy Impact Assessment study should be conducted in the planning stage. **PIA is an assessment of any actual or potential effects that the activity or proposal may have an individual's privacy and the ways in which any adverse effects may be mitigated**. Such studies should also be conducted at different stages of the implementation of a medical record database, e.g. the detailed design of a web-enabled system, the introduction of new applications which access the database."[5]

In March 2001, a session on PIAs was included as part of a Public Seminar on 'E-Privacy in the New Economy', featuring New Zealand's Deputy Commissioner, Blair Stewart.[6]

In his Annual Report for 2000-01, the then Commissioner wrote,

> "the PCPD urged the Health and Welfare Bureau to subject the project to a Privacy Impact Assessment (PIA) at an early stage. A PIA would seek to map the implications of access to lifelong electronic health records.

---

[3] Office of the Privacy Commissioner for Personal Data, E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business, Stage 2: E -Privacy Strategic Planning and privacy Impact Assessment, section 8.4, 2001, at http://www.pcpd.org.hk/english/publications/eprivacy_9.html

[4] http://www.pcpd.org.hk/english/publications/newsletter_2000nov.html.

[5] "1. Privacy Impact Assessment(PIA)", at http://www.pcpd.org.hk/english/infocentre/speech_20001216.html.

[6] http://www.pcpd.org.hk/english/activities/promotion_eprivacy.html. The slide-set can be viewed at: http://www.pcpd.org.hk/misc/stewart/sld001.htm and the text is at: http://www.pcpd.org.hk/english/infocentre/files/stewart.doc.

> On the matter of PIA the PCPD had occasion during the year to advise the Immigration Department on the proposal to replace the current Hong Kong identity card with a smart card. Two issues were brought to the Department's notice."
>
> "Firstly, this technology permits a large amount of personal data to be concentrated in one card. In the wrong hands therefore an individual smart card could represent a personal data bonanza. This immediately raises the issue of security and the attendant risks of unauthorised access to, and use of, the personal data stored in the card and associated back-end databases. With multiple application cards another real danger is that personal data stored in one part of the card could be cross referenced with data stored in another part of the card.
>
> "We felt that it was our responsibility to inform the Immigration Department of these concerns and the possible unintentional consequences for the smart card holder.
>
> "For this reason, and because the smart card would be so widely held, the PCPD suggested that the Immigration Department conduct a PIA to identify the impact of a smart card upon privacy. We were pleased to learn that the Department subsequently accepted this advice and appointed consultants to undertake a PIA study." [7]

In 2001, PIAs were mentioned in s.8 of a Commissioner's Office document 'E-Privacy: A Policy Approach to Building Trust and Confidence in E-Business'. The relevant passages are extracted in Appendix 1 to this document.[8]

In the Annual Report for 2003-04, the then Commissioner, Raymond Tang, said,

> "Over the course of the next year we will embark upon a programme to educate the community, private and public sectors in particular, about Privacy Impact Assessment ("PIA"). PIA has been defined as "the identification of future consequences of a current or proposed action"[9] and implies the adoption of a systematic process that evaluates any project proposal in terms of its impact upon privacy. The position taken by the PCPD is that PIA should become a constituent component of the project planning process.
>
> "PIA has the potential to become a major force in identifying and managing the "downstream" privacy impact of projects, especially those that make use of computer based or surveillance technologies that capture and collect personal data. We will therefore make PIA a focus of our efforts over the year and, in the longer term, move on to consider the related aspect of privacy compliance or the auditing of projects that have been evaluated by PIA".

In 2007, the Commissioner sees a PIA as "an evaluative process for assessing privacy risks associated with proposals that involve the processing and use of personal data".[10]

Tools

The only guidance provided for the conduct of PIAs Hong Kong is provided by the Office of the Privacy Commissioner for Personal Data and found in the Information Book of 2001, E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business,

---

[7] Office of the Privacy Commissioner for Personal Data, Annual Report for 2000-01, at: http://www.pcpd.org.hk/english/publications/overview2001_5.html.

[8] Office of the Privacy Commissioner for Personal Data, Information Book of 2001, *E-Privacy: A Policy Approach to Building Trust and Confidence in E-Business*, at http://www.pcpd.org.hk/english/publications/files/eprivacy_booklet.pdf.

[9] Office of the Privacy Commissioner for Personal Data, Annual Report for 2003-04, at: http://www.pcpd.org.hk/english/publications/overview2004_1.html.

[10] Interview with Allen Ting, Acting Chief Privacy Compliance Officer, Office of the Privacy Commissioner for Personal Data, Hong Kong.

under Stage 2: E -Privacy Strategic Planning and Privacy Impact Assessment.[11] Pertinent extracts are reprinted in Appendix 1.

Completion of PIAs

By Whom?

In his guidance material, the Commissioner states that "There are distinct advantages in outsourcing a PIA study not the least of which is that it lends impartiality to the process**.** This may be critical in influencing consumer or public opinion."[12]

By What Organisations?

The new Hong Kong ID Card was the subject of a PIA at each of four phases between 1999-2000 and 2004.[13] They appear to have been performed for the Immigration Department by at least two and as many as four different consultancy firms. The first report was presented to the Privacy Commissioner for comment during 2000, and was published by the Legislative Council. However it does not appear that the three subsequent PIAs were published.[14]

In a presentation in April 2005 at a conference in Geneva by the then Acting Privacy Commissioner, Tony Lam, the following further examples of PIAs conducted in Hong Kong were mentioned:[15]

- the 'Caller Number Display' feature of telecommunication service;
- 'Electronic Road Pricing' proposal;
- 'Online banking' services.

It is noteworthy that these examples cross over into the private sector.

When and under what circumstances?

The Commissioner's guidance material says that the, "PIA is a process that may be applied to a wide range of E-Business proposals that may be intrusive in terms of reasonable expectations of privacy, or the privacy rights enshrined in the Ordinance. It

---

[11] Hong Kong PIA guidance material may be found at: http://www.pcpd.org.hk/english/publications/eprivacy_9.html.

[12] Office of the Privacy Commissioner for Personal Data, *E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business*, Stage 2: E -Privacy Strategic Planning and privacy Impact Assessment, section 8.5, 2001, at: http://www.pcpd.org.hk/english/publications/eprivacy_9.html.

[13] Reports from the Legislative Council are at:

1. Feb 2001: http://www.legco.gov.hk/yr00-01/english/panels/se/papers/b752e04.pdf.
2. Jul 2002: http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0710cb2-2433-7e.pdf.
3. 2003-04 No reference located.
4. Feb 2005 http://www.legco.gov.hk/yr04-05/english/panels/se/papers/secb2-858-1e.pdf.

The Legislative Council Database on the HKSAR Identity Card Project is at: http://www.legco.gov.hk/database/english/data_se/se-hksar-identity-card-project.htm

[14] Hong Kong Special Administrative Region Identity Card Project - Report on Initial Privacy Impact Assessment' Submitted September 2000, Revised after Client comments, November 2000, Pacific Privacy Pty Ltd http://www.legco.gov.hk/yr00-01/english/fc/esc/papers/esc27e1.pdf

[15] Tony Lam's presentation may be found at slide 22 at: http://www.itu.int/osg/spu/ni/ubiquitous/Presentations/10_lam_dataprotection.pdf

has equal validity applied to a public policy initiative e.g. electronic road pricing, as it has to a corporate initiative e.g. online customer profiling for prospecting purposes."[16]

Review/Approval of PIAs

Oversight Office Review and Acceptance

The Commissioner may provide critique and feedback on PIA reports, but does not play any role such as formal advisor, consultant or inspector.

Public Availability

There are no known examples of published PIA Reports. However, in his guidance material, the Commissioner states that "in the public sector the findings of a PIA study might be incorporated in a public consultation exercise, or policy position statement."[17]

Lessons Learned

Observations on the Quality of PIAs

No information has been located relating to the quality of PIA processes or PIA Reports.

Utility of PIAs in Hong Kong

This is limited to date, but with a couple of beacon cases.

Room for Improvement

Oversight Body

The Privacy Commissioner continues to encourage the conduct of PIAs, and is prepared to assist with critique and feedback.

Central Agency

No central agency has to date played any role in relation to PIAs.

Practitioners

No evidence of the practitioner's perspective was able to be gained during the study.

Directions of PIAs in Hong Kong

No information has been found more recent than the statements in the Annual Report for 2003-04 that "PIA should become a constituent component of the project planning process" and "we will therefore make PIA a focus of our efforts over the year and, in the longer term".

[16] Office of the Privacy Commissioner for Personal Data, *E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business*, Stage 2: E -Privacy Strategic Planning and privacy Impact Assessment, section 8.4, 2001, at: http://www.pcpd.org.hk/english/publications/eprivacy_9.html.

[17] Office of the Privacy Commissioner for Personal Data, *E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business*, Stage 2: E -Privacy Strategic Planning and privacy Impact Assessment, section 8.5, 2001, at http://www.pcpd.org.hk/english/publications/eprivacy_9.html.

In his Annual Report for 2005-06, the current Privacy Commissioner, Roderick Woo, referred to an extensive review being undertaken of the now 10-year-old Ordinance, with the intention that amendments be proposed to the Legislative Council. It is reasonable to expect that some provision relating to PIAs may feature in those proposals.

Research

The following individuals were interviewed:

Office of the Privacy Commissioner (the oversight body):
- Mr Allen Ting, Acting Chief Privacy Compliance Officer, for the Privacy Commissioner for Personal Data
- Mr Stephan Lau, former Privacy Commissioner for Personal Data

In addition, documents provided by the Privacy Commissioner's Office and Legislative Counsel 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.

Appendix 1

Extract from
E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business
Stage 2: E -Privacy Strategic Planning and privacy Impact Assessment[18]

Office of the Privacy Commissioner for Personal Data
Information Book of 2001

Note: *Emphasis added in this document*.

Q3) Is there a clear definition of what a PIA is, and how it differs from other compliance tools such as legal compliance checks and auditing?

8.3 The E-Privacy Strategic Planning process needs to operate in parallel with a Privacy Impact Assessment ("PIA"). In the absence of a common definition, a PIA may be described as **a systematic process that evaluates proposed initiatives or strategic options in terms of their impact upon privacy**. To be effective a PIA needs to be **an integral part of the project planning process rather than an afterthought**. The purpose of this assessment is twofold.

- To identify the potential effects that a project or proposal may have upon personal data privacy e.g. the introduction of a multi-purpose smart card.
- Secondly, to examine how any detrimental effects upon privacy might be mitigated.

8.4 PIA is a process that may be applied to a wide range of E-Business proposals that may be intrusive in terms of reasonable expectations of privacy, or the privacy rights enshrined in the Ordinance. **It has equal validity applied to a public policy initiative** e.g. electronic road pricing, **as it has to a corporate initiative** e.g. online customer profiling for prospecting purposes.

8.5 **A PIA needs to commence at the outset of any planning initiative, strategy or policy proposal**. Although the approach taken to PIA may vary with the context in which it is undertaken that approach should be methodical. Experience indicates that it should begin with definition of the problem or statement of issues. **There are distinct advantages in outsourcing a PIA study not the least of which is that it lends impartiality to the process**. This may be critical in influencing consumer or public opinion. For example, in the public sector the findings of a PIA study might be incorporated in a public consultation exercise, or policy position statement. This suggests that PIA is not an end in itself.

8.6 **The outcome of any PIA should be measured against the influence it exerts upon proposals and strategic decision making**. Ultimately the purpose is to ensure that decision-makers are cognizant of the privacy dimension and work towards decisions that are privacy enhancing.

8.7 PIA has been referred to by a leading figure in the privacy community as **an "early warning system"**. Approached correctly a PIA should ensure that organisations avoid the pitfalls that are implicit in a less disciplined approach to privacy issues. More significantly, as E-Business volumes grow, PIAs will contribute to protecting the image, goodwill and public confidence in those organisations that offer their services online.

[18] at http://www.pcpd.org.hk/english/publications/eprivacy_9.html.

APPENDIX H

Broad Jurisdictional Report for the European Union

CONTENTS

Context

This report examines the broad position to date regarding the use of Privacy Impact Assessments (PIAs) or PIA-like processes within the Member States of the European Union/European Economic Area. This does not purport to be an exhaustive examination of the 27 EU Member States; rather it looks at the existing state of play across the EU generally.

It may perhaps come as no surprise to discover that the use of 'Privacy Impact Assessments' has received relatively minor attention within the EU. An academic literature search generates virtually no material in the English language focused on PIAs in EU Member States; a practitioner literature search does no better. There are occasional mentions; suggestions in passing that the EU might formally adopt some form of PIAs; but no sustained or detailed examination of the European 'state of the art' in English.

There, of course, lies one of the stumbling blocks to this assessment: PIAs as a concept have largely been developed in the Anglophone world – with countries such as New Zealand, Australia and Canada taking the lead. This does not, however, mean that other non-Anglophone countries are not engaged in similar exercises, or are not already working to the same ends; rather it may mean that they simply call that process of assessing privacy risks in advance of engaging in new, or re-engineering old, projects and practices involving personal data, by some other name than PIAs. Indeed, it is entirely possible that they've been doing similar assessment for so long that its rationales and goals are no longer an area of controversy for academics or practitioners.

We are, after all, a union of nations who, in the process of implementing Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive),[1] managed to differ as to our understanding of the meaning of such fundamental data protection definitions as 'data controller,' 'data processor,' 'sensitive data,' 'anonymous data,' 'consent,' 'third party,' 'establishment,' and 'equipment.' In that light, the fact that we might fail to come to a common usage of the term 'PIA' seems hardly surprising, not least given the fact that even in those jurisdictions where the term is used, its definition and underlying understandings are rarely entirely uniform.

In short then, this is a study less concerned with obtaining a view of whether public or private sector bodies in the EU Member States make use of a tool called a 'PIA', than it is with eliciting whether legislators, regulators and public or private sector bodies in the EU Member States are open to, or already engaging with, PIA-type processes.

Legislative and Policy Framework

While there are a number of other EU Directives that contain data privacy elements including the Distance Selling Directive,[2] the E-Commerce Directive[3] the Electronic Signatures Directive,[4] and the Electronic Communications Data Protection Directive,[5]

1 Directive 95/46/EC, 1995 O.J. (L 281) 31-50.

2 Directive 97/7/EC, May 20, 1997, On the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19-27.

3 Directive 2000/31/EC, June 8, 2000, On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1-16.

4 Directive 1999/93/EC, Dec. 13, 1999, On a Community Framework for Electronic Signatures, 2000 O.J. (L 013) 12-20.

Directive 95/46/EC provides the broad framework upon which the Member States of the EU (and the EEA States) have developed their data privacy regimes.

The Directive provides that Member States should have an independent supervisory authority, or authorities authorised to receive and investigate complaints. It further requires that the supervisory authority or authorities should have effective powers of intervention, including that of delivering opinions before processing operations are carried out. While the Directive is silent on the issue of 'Privacy Impact Assessments,' in order to enable the supervisory authority or authorities' power of pre-processing intervention, Article 20 of the Directive requires that processing operations likely to present specific risks to the rights and freedoms of data subjects should be examined prior to their start – which the Directive describes as 'prior checking'.

> **Article 20**
>
> **Prior checking**
>
> 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
>
> 2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
>
> 3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

However, as Member States are given the discretion to determine which activities present a specific risk to the rights and freedoms of individuals and thus require prior checking, the extent to which this provision is clearly incorporated into law by Member States and acted upon as policy by their supervisory authorities varies. For example, 'prior checking', in certain circumstances, was clearly envisaged by the UK Government in its paper describing the Government's proposals for implementing the Data Protection Directive:

> **Prior checking**
> 5.13 The Government is considering which categories of processing operation should be subject to the prior checking system required by article 20. It wishes to limit them to the minimum consistent with the need to provide adequate protection for individuals in the light of the tight criteria set out in the Directive. No decisions have yet been taken, but the Government is currently considering whether there is a case for prior checking some processing operations involving data matching, genetic data and private investigation activities. The proposed prior checking mechanism is described in paragraph 6.10.[6]
>
> […]
>
> **Prior checking**
> 6.10 Under the present law processing may lawfully begin once the application for registration has been made. The new law will preserve this provision for the great majority of processing. However, those operations subject to prior checking (see

[5] Directive 2002/58/EC, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37-47.

[6] *Data Protection: The Government's proposals.* Home Office CM3725, (1997) Chapter 5: Notification./Registration.

> paragraph 5.13) will not be allowed to start until they have been checked by the supervisory authority. The supervisory authority will be required to carry out that check and give its opinion to the controller within, say, 15 working days of receiving the application. The opinion may take the form of a notification to the controller that the supervisory authority is minded to issue an enforcement notice; or a statement to the effect that it does not intend to take any further action in the context of the prior checking exercise. In either case, the processing may go ahead. If the controller decides to go ahead, he will of course be at risk of subsequent challenge from the supervisory authority for any breach of the Act. [7]

Section 22 of the UK Data Protection Act 1998 provides for a version of 'prior checking' by requiring that, as part of the notification process, certain processing might be assessed by the Information Commissioner for compliance with the provisions of the Act before the processing begins – preliminary assessment. The type of processing must specified in an Order made by the Secretary of State, if it is considered that processing would be particularly likely:

- to cause substantial damage or substantial distress to data subjects; or
- otherwise significantly to prejudice the rights and freedoms of data subjects.

Controllers wishing to process material in the preliminary assessment categories would be required to notify the Commissioner as with any other processing. They would then have to wait for a period of up to 28 days before starting processing to permit the Commissioner to give an opinion about likely compliance with the Act. In its White Paper of July 1997 the UK government identified 3 possible categories of processing that might be covered by 'preliminary assessment':

- data matching;
- processing involving genetic data;
- processing by private investigators.[8]

However, to date, no order has been yet been made in the UK, and the previous UK Information Commissioner suggested that "no 'assessable processing' should be designated".[9]

As outlined below, other Member States (and indeed the EU itself) have been more inclined to adopt a "prior check" or "prior authorisation" regime for particular types of processing.

Prior Checking in the European Union

In most cases, where Member States have implemented 'prior checking', the primary legislation defines the categories of processing operations that will be subject to prior checking, but sometimes the law provides that secondary legislation will define which processing operations should be subject to prior checking. The degree to which prior checking is used across the Member States varies widely. Table 1 is drawn from the following sources, the Article 29 Working Party's *Vademecum on Notification*

---

7 *Ibid*. Chapter 6: Enforcement.

8 *Data Protection Act 1998: Consultation Paper on Subordinate Legislation*, Home Office (1998), para. 20.

9 Cited in: Foundation for Information Policy Research, *Children's Databases – Safety and Privacy: A Report for the Information Commissioner* (March/August 2006) at p.187. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrens_personal_information.pdf.

Requirements; documentation available from the supervisory authorities' websites; academic and practitioner literature; and personal communications.

Table 1 Prior Checking uptake in the European Union Member States

Country	Prior checking or prior authorisation or permit required	Legislation, if applicable.
Austria	Processing sensitive data Processing data concerning offences and criminal convictions. Processing data to obtain information on a data subject's creditworthiness All "interconnections" between files (databases). All "combinations" of data (data matching, results of data sharing).	s.18, Act Concerning the Protection of Personal Data 2000 (Datenschutzgesetz 2000)
Belgium	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Bulgaria	Several sources suggest Bulgaria does not have prior checking as envisaged under Article 20, Directive 95/46/EC.[10] Art.15 & 16 Bulgarian Personal Data Protection Act refer to some form of prior checking.	Possibly Art.15 & 16 Bulgarian Personal Data Protection Act
Cyprus	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Czech Republic	Not known[11]	N/A
Denmark	Processing sensitive data Processing data concerning offences and criminal convictions. Use of files excluding individuals from a right or benefit of contract (blacklists). Processing data to obtain information on a data subject's creditworthiness Processing for the purpose of professional assistance in connection with staff recruitment Processing for the purpose of operating legal information systems.	s.50, Act on Processing of Personal Data
Estonia	No prior checking as envisaged under Article 20,	N/A

[10] See Beyleveld, D., Townend, D., Rouillé-Mirza, S. & Wright, J. (eds.) (2004). *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Ashgate at p.187; Commission Staff Working Document, *Bulgaria - May 2006 Monitoring Report* COM (2006) 214 final, p.19.

[11] In the Article 29 Working Party's *Vademecum on Notification Requirements* (03/07/06) it stated that the Czech Republic legislation does provide for prior checking, but it is currently not possible to verify this from available documentation.

	Directive 95/46/EC.	
Finland	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
France	Processing of the national identification number ("NIR", or social security number) Use of sensitive data (with exceptions) Interconnection of files held by different controllers for different purposes; Processing operations with a purpose to select individuals for the benefit of a right, of a service or of a contract when they are not excluded from this benefit by law or regulation, e.g. files which list the names of bad debtors, used to avoid the granting of credit to individuals who have occasionally failed to pay their debts; and more generally all forms of "blacklists"; Processing operations on biometric data that are necessary to control the identity of individuals, Processing operations on genetic data, Processing operations on criminal data, Processing personal data concerning offences and criminal convictions.	Art.25, Data Protection Act (Loi Informatique et Libertés) 1978 as amended France effectively had a system of prior checking before implementation of the EU Directive, where the public sector was subject to prior checking procedures
Germany (Federal)	Where automated processing operations pose particular/specific risks for the rights and liberties of the data subjects, especially • use of sensitive personal data or • where the purpose of the processing of personal data is to evaluate the data subject's personality including his abilities, his performance or his behaviour, unless a legal obligation applies or the data subject's consent has been obtained or the collection, processing or use furthers the object of a contractual relationship or a quasi-contractual relationship of trust with the data subject.	s.4d Federal Data Protection Act (Bundesdatenschutzgesetz)
Germany (Land Berlin)	The Land Berlin has similar rules to those of the German Federal data protection law, but requires prior checking in order to detect possible as opposed to specific risks to informational self-determination. The wording of this legislation resembles most closely that of PIA processes.	s.5 (3) Berlin Data Protection Act (Berliner Datenschutzgesetz)
Greece	Processing sensitive data All "interconnections" between files. All "combinations" of data.	Arts. 7-8, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended)

Hungary	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Ireland	Provided for, but categories of data not defined in primary legislation, no secondary legislation to date	s.12A, Data Protection Act
Italy	Processing likely to present specific risks to data subjects' fundamental rights and freedoms and dignity on account of the nature of the data, the arrangements applying to the processing, or the effects the latter may produce.	s17, Legislative Decree no. 196 of 30 June 2003 Personal Data Protection Code
Latvia	It appears that all processing is potentially subject to prior checking.[12]	Art.22(2), Personal Data Protection Act 2000
Lithuania	Processing of sensitive personal data by automated means Processing of public data files by automated means Processing carried out by a data processor on behalf of a data controller of the information systems of state registers or state and municipal institutions Processing of personal data in the course of scientific research on condition without the consent of the data subject Processing of personal data to evaluate of a person's solvency and to manage their debt Processing of personal data for the statistical or research purposes where data subjects are not informed	Art.26, Law on Legal Protection of Personal Data
Luxembourg	Most data processing operations related to sensitive data, video-surveillance, surveillance in the workplace by the employer, interconnection of data, use of personal data for other purposes than those for which they have been collected, data processing related to credit and solvency of the data subjects.	Art.14, Loi sur la protection des données (as amended)
Malta	Processing of personal data that involves particular risks of improper interference with the rights and freedoms of data subjects, categories of data not defined in primary legislation.	s.34 Data Protection Act 2003
Netherlands	Processing a number identifying persons for a purpose other than the one for which the number is specifically intended with the aim of linking the data together with data processed by other responsible parties, unless otherwise permitted. Recording data on the basis of data controller's own observations without informing the data subjects thereof. Processing data on criminal behaviour or on unlawful or objectionable conduct for third parties other than under	Art. 31, Personal Data Protection Act 2000

[12] According to Beyleveld, D. et al; supra at p.180.

	the terms of a licence issued under the Private Security Organisations and Investigation Bureaus Act.	
Poland	Data filing systems containing the following data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions or penalty, fines and other decisions issued in court or administrative proceedings.	Art. 46a Act of 29 August 1997 on the Protection of Personal Data (as amended)[13]
Portugal	Processing sensitive data Processing personal data concerning offences and criminal convictions. Processing of personal data relating to credit and the solvency of the data subjects The combination of personal data not provided for in a legal provision	Art. 28, Protection of Personal Data Act 1998 (Lei da Protecção de Dados Pessoais)
Romania	No prior checking as envisaged under Article 20, Directive 95/46/EC	N/A
Slovakia	Processing of personal data for protection of statutory rights and legitimate interests of the controller or the third party without data subjects consent Some types of processing of biometric data	s.27, Act No. 428/2002 Coll. on Protection of Personal Data
Slovenia	Not known	N/A
Spain	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Sweden	Government can issue regulations providing that processing of personal data that has particular risks of improper interference with the rights and freedoms of data subjects shall be notified for preliminary examination. Regulations have been issued by the Government in: • the Personal Data Ordinance (processing of personal data concerning hereditary disposition derived from genetic investigation) • the Police Data Ordinance, • the Ordinance on personal data processing by tax authorities' when assisting in criminal investigations • the Ordinance on personal data processing in the Customs' activity regarding fight against crimes	s.41, Personal Data Act

[13] This is the position stated in the Article 29 Working Party's *Vademecum on Notification Requirements* (03/07/06), but it is difficult to verify from available documentation.

UK	Provided for, but categories of data not defined in primary legislation, no secondary legislation to date.	s.22, Data Protection Act 1998

The Differences between Prior Checking and PIAs

Some of these forms of prior checking may require data controllers wishing to engage in relevant processing to undertake a similar style and degree of analysis of new or adapted projects and processes as is found with the Privacy Impact Assessments. However, use of prior checking is usually limited to specific circumstances whether there is either:

- processing of certain types of sensitive data (as defined in the Directive);
- processing of other critical personal data (e.g. national identity numbers, biometric data, personal financial information, data used for 'blacklisting');
- data matching/data sharing.

Among the apparent exceptions to this rule are Latvia, where from the translated text of the Latvian Personal Data Protection Act 2000, it appears that all new data processing is potentially subject to prior checking, and the German Land of Berlin. The latter's prior checking mechanism in s 5(3) of the Berliner Datenschutzgesetz (BlnDSG) translates approximately as:

> (3) Before a decision on the use of, or a significant change in, automated data processing, appropriate technical and organisational measures should be determined on the basis of a risk analysis and a security evaluation. Where the data is processed is for employment purposes, is subject to official secrecy, or collected for the prosecution of criminal offences, a preliminary inspection of potential dangers to the right to informational self-determination is required. Where, despite the use of practicable security measures, unacceptable risks remain which cannot be overcome by [appropriate technical and organizational measures] and the [confidentiality, integrity, availability, authenticity, nature and author of revisions, or transparency] guaranteed, the processing should not take place. [14]

This appears broader in scope than the basic prior checking provisions found in other jurisdictions, including that of the German Federal Data Protection Act (Bundesdatenschutzgesetz), and appears to bear closer similarity to the PIA processes reviewed elsewhere in this Study, in terms of the expectation of the use of risk and security analyses prior to the adoption of new or revised forms of data processing, and the preemptive consideration of appropriate mitigation strategies.

[14] (3) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Dazu gehört bei Verfahren, mit denen Daten verarbeitet werden, die einen Berufs- oder besonderen Amtsgeheimnis unterliegen oder die zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden, eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung. Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 2 oder eine Modifizierung der automatisierten Datenverarbeitung verhindert werden können, darf ein Verfahren nicht eingesetzt werden.

Elements of the French 'prior checking/assessment' process also relate to elements of a PIA process, not least in the ability of the public to access notification information, the details of decisions made by CNIL with regard to the conditions required if 'risky' processing is to be allowed, as well as the reasons why 'risky' processing has not been allowed. However, in CNIL's 'prior checking' regime both the risk assessment and the publicity are facilitated by the supervisory authority rather than by the organisation carrying out the processing.

In general, across the Member States using 'prior checking' or similar mechanisms, such as 'prior authorisation' and licensing, the scope of such 'prior checking' appears to be narrower than that of PIAs, where the tendency is for a holistic privacy risk assessment rather than a basic assessment of compliance with data protection law, to be undertaken.

Previous work undertaken for the UK Information Commissioner, including the Foundation for Information Policy Research's *Children's Databases – Safety and Privacy: A Report for the Information Commissioner,* written in 2006,[15] has suggested that the UK should reconsider its current position on 'prior checking' for certain categories of personal data processing. It is suggested here that encouraging the widespread use of PIAs could:

- facilitate the process of 'prior checking' by allowing the supervisory authority to draw upon the results of PIAs incorporated into organisational processes, such as Threat Risk Assessments for new or redesigned projects;
- broaden the pool of organisational privacy understanding and expertise such that organisations will be more readily aware of the need for 'prior checking' when it is appropriate, and better able to supply the supervisory authority with appropriate information about the project/process for an appropriate prior checking assessment or decision to be made efficiently.

It is clear, however, that while supervisory authority 'prior checking' in specific circumstances has its place in a data privacy regime, in most circumstances that process is not currently synonymous with the PIA process, as it is understood in jurisdictions, such as Canada, Australia, and New Zealand.

Adoption of PIAs in the European Union Member States

While some form of 'prior checking' is provided for in legislation, and sometimes actively used, in at least 16 of the Member States, the use of PIAs of the type reviewed by this Study,in jurisdictions such as Canada, Australia, and NZ appears rare. Two Member States that have begun to explore this avenue are Finland and Ireland. Both are at a very early stage in their development work.

The Office of the Data Protection Ombudsman, Finland, has begun preliminary work on developing a PIA questionnaire, and early indications are that both public and private sector organisations would be expected to undertake PIAs, although it is unclear whether this would be at the discretion of the organisations, or whether it would be compulsory. The suggested Finnish model seems to be largely based upon, and to resemble the PIA models found in Canada, Australia and NZ.

In Ireland, the Irish Data Protection Commissioner's Office has developed policy guidance in relation to biometrics in the workplace and schools where they recommend

[15] Supra at n.9.

undertaking a Privacy Impact Assessment. The Office does not offer a template per se, but in the context of biometrics has provided a list of a range of issues that could be considered in a PIA (see below). The Data Protection Commissioner's Office integrates the undertaking of a PIA into advice it issues to organisations where it would be of benefit, and suggests that this has led to increased awareness of the need to take privacy concerns into account in decision-making processes.

> Irish Data Protection Commissioner's Office, *Biometrics in the workplace*[16]
>
> **[…]**
>
> **8. Privacy Impact Assessment.**
>
> The Data Protection Commissioner cannot give a general approval or condemnation of biometric systems. Each system must be judged in respect of the situation in which it is used. A case-by-case judgement is required. With that in mind, the Commissioner encourages employers to take the above guidance into account if considering introducing any biometric system.
>
> Before an employer installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out. An employer who properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against an employer by the Commissioner, or may expose an employer to a claim for damages from an employee. Data protection responsibility and liability rests with the employer, not with the person who has supplied the system (except where that person also acts as a data processor on behalf of the employer).
>
> Some of the points that might be included in a Privacy Impact Assessment are:
>
> - Do I have a time management and/or access control system in place?
> - Why do I feel I need to replace it?
> - What problems are there with the system?
> - Are these problems a result of poor administration of the system or an inherent design problem?
> - Have I examined a number of types of system that are available?
> - Will the non-biometric systems perform the required tasks adequately?
> - Do I need a biometric system?
> - If so, why kind do I need?
> - Do I need a system that identifies employees as opposed to a verification system?
> - Do I need a central database?
> - If so, what is wrong with a system that does not use a central database?
> - What is the biometric system required to achieve for me?
> - Is it for time management purposes and/or for access control purposes?
> - How accurate shall the data be?
> - What procedures are used to ensure accuracy of data?
> - Will the data require updating?
> - How will the information on it be secured?
> - Who shall have access to the data or to logs?
> - Why, when and how shall such access be permitted?
> - What constitutes an abuse of the system by an employee?

[16] http://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm

- What procedures shall I put in place to deal with abuse?
- What legal basis do I have for requiring employees to participate?
- Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?
- If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?
- How shall I inform employees about the system?
- What information about the system need I provide to employees?
- Would I be happy if I was an employee asked to use such a system?
- How will I ensure that employees who are unable to provide biometric data because of a disability, for example, are not discriminated against by being required to operate a different system, or otherwise?
- What is my retention policy on biometric data?
- Can I justify the retention period in my retention policy?
- Do I have a comprehensive data retention policy?
- Have I updated this policy to take account of the introduction of a biometric system for staff?

As such, the development of PIAs in the Member States is at a relatively early stage. While there is interest in the concept of PIAs and the role that they could play within national data protection regimes and in privacy protection more widely, there are currently no completed tools, and there are limited legislative or policy frameworks in place to support their use. In most Member States it appears that the scope of 'prior checking' and similar functions in national legislation would not extend to justifying the broad introduction of PIAs, particularly as a compulsory requirement. As such, it is likely that where Member States' supervisory agencies wish to see PIAs adopted as part of their national data protection regime, this will develop out of persuading public and private sectors to adopt PIAs as an issue of policy rather than via legislation. In the public sector, the desire for accountability, efficient management and effective incorporation of Threat/Risk Assessments into key decision-making processes should aid in uptake. The fact that major European corporations such as Philips, Vodafone and others have adopted such strategies, and that these are seen as potentially conferring competitive advantage, may mean that at least some parts of the private sector will also be open to such developments

Research

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

Berlin Office for Data Protection and Freedom of Information
Berliner Beauftragter für Datenschutz und Informationsfreiheit

- Alexander Dix, Commissioner

Dutch Data Protection Authority
College Bescherming Persoonsgegevens (CBP)

- Dr. Lynsey Dubbeld

Irish Data Protection Commissioner's Office

- Ciara M. O'Sullivan

French Data Protection Authority
La Commission Nationale de l'Informatique et des Libertés (CNIL)

- Marie Georges, Counsellor for the President for Advanced Studies, Development and Cooperation.

The Norwegian Data Inspectorate

Datatilsynet

- Astrid Flesland, Senior Legal Adviser

Finnish Office of Data Protection Ombudsman
Tietosuojavaltuutetun toimisto

- Reijo Aarnio, Data Protection Ombudsman

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

- National legislation and unofficial translations
- Webpages describing prior checking processes

Additional materials

Foundation for Information Policy Research, Children's Databases – Safety and Privacy: A Report for the Information Commissioner (March/August 2006)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrens_personal_information.pdf/

Article 29 Working Party, Vademecum on Notification Requirements (03/07/06)
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-vademecum.doc.

Beyleveld, D., Townend, D., Rouillé-Mirza, S. & Wright, J. (eds.) (2004). *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Ashgate.

D. Korff. "Study on Implementation of Data Protection Directive – Comparative Summary of National Laws" (2003)
http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf

APPENDIX I

PIA Templates and Guides by Jurisdiction

I. PIA GUIDANCE

DEFINITIONS

Guidance Type	Description
Guide	Comprehensive guide or handbook, describing process in detail
Process Overview	Short overview of the process or template
Report Outline	Annotated Table of Contents, describing what should be included in the final report.

COUNTRY	TYPE	PUBLISHED MATERIAL
North America		
United States of America	Guide	**National Government**, Office of Management and Budget, *E-Government Act Section 208 Implementation Guidance*, September, 2003, at: http://www.whitehouse.gov/omb/memoranda/m03-22.html Several departments also have their own guides, most notably, the Department of Homeland Security. *Privacy Impact Assessments: official guidance, 2007*, at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf
Canada		
	Process Overview	**National Government**, *Privacy Impact Assessment Policy*, Treasury Board of Canada Secretariat at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piap-pefr_e.rtf
	Guide	*PIA Guidelines: A Framework to Manage Privacy Risks*, Treasury Board of Canada Secretariat, 2002, at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/piapg-pefrld_e.rtf
	Supplement	Report on PIA Best Practices, Treasury Board of Canada Secretariat, 2003, at http://www.tbs-sct.gc.ca/pgol-pged/pia-best/pia-best00_e.asp
	Audit Guide	[For Internal Auditors] *Privacy Impact Assessment Audit Guide*, Treasury Board of Canada Secretariat, 2004, at: http://www.tbs-sct.gc.ca/ia-vi/policies-politiques/pia-efvp/pia-efvp_e.pd f
	Background	PIA e-learning tool, Treasury Board of Canada Secretariat, 2003, at: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a_e.asp
	Process Overview	**British Columbia**, Ministry of Labour and Citizens' Services. *Privacy Impact Assessment Process,* 2006, at: http://www.lcs.gov.bc.ca/privacyaccess/PIA/PIAprocess.htm
	Process Overview	**Alberta**, (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 Note: an alternative PIA process and templates are used by a number of ministries, as described in the appended Alberta Jurisdiction Report. They are not available publicly on the internet.
	Guide	**Ontario**. Management Board Secretariat, Information and Privacy Office. *Privacy Impact Assessment: a User's Guide,* 2001 at: http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf and Ministry of Government Services, *PIA Screening Tool*, (undated) at: http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.pdf

Asia-Pacific		
Australia	Guide	**National Government**, Office of the Privacy Commissioner. *Privacy Impact Assessment Guide,* 2006, at: http://www.privacy.gov.au/publications/pia06/index.html
	Guide	**Victoria**, Office of the Privacy Commissioner of Victoria, Privacy Impact Assessment Guide, 2004, at: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf
New Zealand	Guide	Office of the New Zealand Privacy Commissioner. *Privacy Impact Assessment Handbook,* 2002 http://www.privacy.org.nz/filestore/docfiles/48638065.pdf
Hong Kong	Process Overview	Office of the Privacy Commissioner for Personal Data, Information Book, *E-Privacy: A Policy Approach to Building Trust and Confidence In E-Business*, under Stage 2: E -Privacy Strategic Planning and Privacy Impact Assessment, 2001, at http://www.pcpd.org.hk/english/publications/eprivacy_9.html

II. PIA TEMPLATES

Template Type	Description
Compliance Checklist	List of questions, organized like the governing statute, with yes/no boxes to indicate compliance with provisions
Annotated Compliance Checklist	Same as above, but guidance is provided on answering the questions and there may be an opportunity to explain answers
Screening Checklist	A list with Yes/No boxes or tick boxes containing questions to determine whether a PIA is necessary
Report Outline	Annotated Table of Contents, describing what should be included in a PIA final report.

COUNTRY/ REGION	TYPE	PUBLISHED MATERIAL
North America		
United States		**National Government**, Department of Homeland Security. *Privacy Impact Assessments: official guidance,* 2007
Canada	Annotated Report Outline	**National Government**, PIA Report Template Treasury Board of Canada Secretariat, 2002, at: http://www.tbs-sct.gc.ca/pgol-pged/ppia-epfvp/prelim-temp-modl/prelim-temp-modl00_e.asp
	Annotated Compliance Checklist	**British Columbia**, Ministry of Labour and Citizens' Services. *Privacy Impact Assessment Process,* 2006, at: http://www.mser.gov.bc.ca/privacyaccess/PIA/PiaTemplateRevisedMay06.doc
	Annotated Compliance Checklist	**Alberta**, Office of the Information and Privacy Commissioner of Alberta, *PIAs, Template*, at: http://www.oipc.ab.ca/pia/template.cfm Note: an alternative PIA process and templates are used by a number of ministries, as described in the appended Alberta Jurisdiction Report. They are not available publicly on the internet.
	Screening Checklist	**Ontario**, Ministry of Government Services, Corporate Access and Privacy Office. *Privacy Impact Assessment Screening Tool*, at: http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.pdf
Asia-Pacific		
Australia	Annotated Checklist	**National Government**, Module E, IPP Compliance Checklist, in the PIA Guide contains a Compliance Checklist, at http://www.privacy.gov.au/publications/pia06/mod-e.html
	Screening Checklist	**New South Wales**, Privacy New South Wales has an initial, screening tool: *Checklist – Identifying Privacy Issues Early*, Privacy NSW Privacy Essentials, No 3, April 2004, at: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/privacyessentials_03_2005.pdf/$file/privacyessentials_03_2005.pdf
New Zealand		No template but there is an annotated Table of Contents for a PIA report in the *Privacy Impact Assessment Handbook*
Hong Kong		No template