Privacy Impact Assessments:

International Study of their Application and Effects

October, 2007

Linden Consulting, Inc.

Prepared for
Information Commissioner's Office
United Kingdom

Privacy Impact Assessments:
International Study of their Application and Effects

CONTENTS

ACKNOWLEDGEMENTS

The project team contributing to this report brings together a range of expertise from the UK, Canada and Australia.

Leading the study and authoring the report were Dr. Colin Bennett and Robin Bayley, Directors and Principals of Linden Consulting Inc., Privacy and Policy Advisors, Victoria, Canada.

Research was conducted by team members as follows:

Jurisdiction	Researcher
Australia (national government, states and territories), New Zealand, Hong Kong	*Dr. Roger Clarke*, Principal, Xamax Consultancy Pty Ltd, Canberra, Australia
British Columbia and Alberta (Canada)	*Robin Bayley*, President and Principal, Linden Consulting, Inc., Victoria, Canada
United States of America	*Dr. Colin Bennett*, Professor, Political Science, University of Victoria and Principal, Linden Consulting, Inc., Victoria, Canada
Canada (national government), Ontario (Canada) and selected European states	*Andrew Charlesworth*, Senior Research Fellow, Law School, Bristol University, UK

Each researcher authored the corresponding jurisdiction reports appended.

Review and feedback on this report was provided by all researchers and Dr. Adam Warren, Department of Information Science, Loughborough University.

The team would like to acknowledge the cooperation and participation of the many individuals who were interviewed. Without exception, they were generous with their time, thoughtful and forthcoming. They provided their informed opinions, without which the Lessons Learned section of this report could not have been written. They also had the courage to share examples of the perceived shortcomings of PIA processes. Interviewees were generally enthusiastic about the project, interested in the results and demonstrated a spirit of cooperation that marks the field of privacy regulation internationally.

A complete list of those who were interviewed according to the Framework for Analysis (Appendix A) is provided in Appendix B along with their organisation name and type. Many other people provided information for the report in more informal ways.

EXECUTIVE SUMMARY

This report is the product of an international study into the use, practice and utility of Privacy Impact Assessments (PIA) in order to identify lessons that could be applied in the United Kingdom. The study was conducted for the Office of the Information Commissioner of the United Kingdom. Reviews of legislation, policy and PIA tools were conducted for the United States of America, New Zealand, Hong Kong, Australia and Canada (including states and pertinent provinces). In these jurisdictions, primary research was also undertaken through interviews with individuals in data protection and privacy oversight bodies, in central government agencies as well as with those who had conducted or were responsible for the conduct of PIAs. Less comprehensive research was also undertaken with regard to the jurisdictions of the European Union.

PIAs are not used in all jurisdictions with data or privacy protection regulation. They tend to be confined to English-speaking countries and to those which have enacted “privacy” rather than “data protection” statutes. Many PIA processes were developed and implemented in the late 1990s and early 2000s, often in conjunction with electronic government initiatives or as implementation tools for fairly recent data or privacy protection laws. They are, therefore, more commonly applied in the public sector than the private sector. Along with other self-regulatory, regulatory and technology initiatives, they represent another instrument within the ’toolkit’ of the privacy regulator.

The general conclusions of this survey are as follows:

- PIAs are a good idea and are increasingly recognised as such by privacy commissioners, government agencies, private corporations and privacy advocates. They help to address the increasing concerns about privacy within advanced industrial societies.
- PIAs have been spreading around the advanced industrial world as a result of: legislative requirements; policy guidance by central government agencies; recommendations by privacy and data protection commissioners; and recognition by organisations that PIAs can expose and mitigate privacy risks, avoid adverse publicity, save money, develop an organisational culture sensitive to privacy, build trust and assist with legal compliance.
- The early experience has been evaluated in several jurisdictions, and lessons are being drawn about the most valuable ways to encourage their completion. In this respect, the decision by the ICO to embark on this initiative for the UK is very timely, and in the context of the European Union, pioneering.
- To be valuable, PIAs need to offer a prospective identification of privacy risks *before* systems and programmes are put in place. In every jurisdiction, PIA processes have been designed to be prospective.
- Many exercises which are called PIAs are, however, little more than legal compliance checks. To be meaningful, PIAs have to consider privacy risks in a wider framework which takes into account the broader set of community values and expectations about privacy.
- PIAs are more than the end-product or statement. They refer to an entire process of assessment of privacy risks. Often, the final report or statement, if indeed published, offers a deceptive impression of the nature, scope and depth of the assessment exercise. A simple report does not necessarily indicate a simple assessment. A detailed report does not necessarily reflect a detailed

assessment. Reports also do not necessarily reveal the changes made to the initiative during the PIA process.

- PIAs are only valuable if they have, and are perceived to have, the potential to alter proposed initiatives in order to mitigate privacy risks. Where they are conducted in a mechanical fashion for the purposes of satisfying a legislative or bureaucratic requirement, they are often regarded as exercises in legitimation rather than risk assessment.
- PIA processes vary across a number of dimensions: the levels of prescription, the application, the circumstances that might trigger PIAs, the breadth of the PIA exercise, the agents who conduct PIAs, the timing, the process or review and approval and the level of public accountability and transparency.
- In most jurisdictions where law or policy require or highly recommend that PIAs be conducted, an official PIA template, format or other tool to describe how they should be conducted, is provided. However, there is no simple formula for the conduct of a PIA. Each PIA should be dictated by the specific institutional, technological, and programmatic context of the initiative in question. A mechanical “checklist” alone does not capture the broader social, political and ethical implications of many initiatives. Any PIA requires judgment.
- Therefore the scope and depth of the PIA needs to be sensitive to a number or crucial variables: the size of the organisation; the sensitivity of the personal data; the forms of risk; the intrusiveness of the technology. A PIA screening process is commonly used to determine whether a PIA is required, and if so, the form it should take.

PIAs appear to be more effective:

- When they are part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes, as is common with other forms of threat/risk assessment. Even within the same jurisdiction, internal organisational policies or practices of like organisations differ, often depending on the will and resources of the area charged with privacy protection.
- When the individuals charged with completing PIAs not only have good programme knowledge, but also have access to expertise from a variety of perspectives − privacy law and practice, information security, records management, and other functional specialists as appropriate. Universally, the organisation whose initiative is being assessed is responsible for the conduct of PIAs. However, there is also a tendency toward the increasing involvement of external consultants.
- Where there is a process of formal or informal external review either by central agencies or privacy oversight bodies.
- Where there is external consultation with outsiders affected by the initiative. PIA processes differ in the degree to which external consultation is advised or required. Most PIA guidance suggests that key project stakeholders should be consulted, including regulators, other agencies, third party vendors and service providers, and others directly affected by the project reviewed. Public consultation is often advised. The form public consultation takes usually varies according to the scope and privacy intrusiveness of the project.

- When there is transparency, and the resulting statements or reports are published. Openness of process and output enhances trust in the initiative being proposed. However, even when rules require PIAs to be listed, published, or otherwise made publicly available, this is not always done.

In the UK, because there is no legislative mandate to conduct PIAs, and because the Commissioner can only recommend their completion, provision of assistance and guidance to those conducting PIAs will be critical in having the PIA adopted. The PIA process itself should be one that practitioners believe is of value to their organisations and the payback should be commensurate with the resources expended. With these lessons in mind, the accompanying Handbook for the United Kingdom is premised on the following assumptions.

- PIAs should be comprehensive risk assessment exercises, using privacy concepts beyond those entailed in data protection legislation.
- They should be more process-oriented than output-oriented.
- Where possible they should be integrated into existing business and management processes, rather than seen as 'add-ons.'
- A screening tool should determine the scale of the PIA to be conducted. The PIA process should be flexible, allowing for the level of resources expended being commensurate with the privacy risks.
- The guidance should indicate the circumstances when full PIAs may be necessary, where smaller-scale PIAs may be appropriate or where PIAs are unnecessary.
- The conduct of PIAs should be transparent and accountable. The process should include external consultation where appropriate, at a point where the direction of the initiative may be influenced, and reports should be published or otherwise made available.
- After a review of the Handbook, the guidance and practical experience, the ICO should consider the circumstances under which PIAs might be required by legislation in the UK (as they are in some other jurisdictions), and make appropriate recommendations.

I. INTRODUCTION

Study Method

This report is the product of an international study of the use, practice and utility of PIAs in order to identify lessons that could be applied in the United Kingdom. The team examined experience in all jurisdictions in which we were cognisant of extensive of PIAs: Australia, Canada, New Zealand, Hong Kong and the United States. In Australia, Canada, New Zealand, Hong Kong and the US, reviews of legislation, policy and PIA tools were conducted. In these jurisdictions, interviews were also conducted with individuals in key positions in data protection oversight offices, non-governmental organisations, and government agencies who had conducted or were responsible for the conduct of PIAs. In addition, a number of European countries were scanned for evidence of PIAs, similar instruments to PIAs or any plans to develop them.

Responsibility for conducting the research was split among team members, but they used a common Framework for Analysis. Researchers developed their interview questions, based on their initial research or knowledge of the jurisdiction, and interviews were designed primarily to confirm or fill in gaps in the Framework for Analysis that had not been readily filled from documentary evidence. The jurisdiction reports in Appendix A are organised according to this same framework.

Interviews were conducted in person and by phone from June through August, 2007, depending on availability of subjects. All interviewees were asked if they could be cited on the record, although jurisdiction reports most frequently cite the organisational affiliation of the individual interviewed. The list of interviewees in Appendix C names all those individuals with whom interviews were conducted. In addition to interviews, a number of more informal telephone calls and e-mails were sent to other individuals to confirm facts or request publications. These individuals are not named, but records have been kept for audit purposes.

A significant amount of research was conducted on the internet, from websites of privacy oversight offices and central agencies, where the PIA policy, legislation, templates and guidance material were often published. Reference was also made to annual reports, legislative reviews, media reports and other general material.

Terminology

Defining PIAs

It is perhaps easier to define PIAs initially in terms of what they are not. PIAs are not simply legal compliance checks motivated by the question: “If we did X, would we be in compliance with the law and the fair information principles upon which the law is based?” After all, such questions have been asked for as long as data protection laws have been in existence. Neither are they the same as privacy audits, the detailed analysis of systems that are already in place against a prevailing legal, management or technology standard.

There seem to be two common assumptions about the nature of PIAs. First, they need to be prospective, and are generally viewed as most useful for new programmes, services or technologies. According to David Flaherty, they should occur in advance of the application or introduction to raise “privacy alarms at an early stage in an

organisation's planning process."[1] They must therefore have the potential to identify and mitigate risks, as well as to modify plans accordingly. It is an "early warning system for management and responsible Ministers and organisations."[2] According to Blair Stewart, "the privacy impact assessment process …is not usually predicated on an examination of an agency's current practices but is directed towards a proposal for the future."[3]

Secondly, and consequently, PIAs should raise bigger issues, beyond whether a particular proposal would be legally compliant. Stewart contends that "in large measure, PIAs are directed not simply towards issues of legal compliance but the policy choices involved in answering the questions 'ought we to do this?' and 'is there another, better way of doing this?'"[4] If properly conducted, therefore, PIAs should have the potential to modify, and in rare cases stop, the introduction of intrusive initiatives and schemes. They should force organisations to think about the larger social questions concerning the balance between individual privacy, and the needs of public and private organisations.

Legal compliance is, therefore, one of several criteria that need to be addressed in a larger process of risk assessment. Those larger questions include the "moral and ethical issues posed by whatever is being proposed."[5] Many projects might be technically compliant with law, but may raise significant concern, even resistance, in certain societies or among certain publics.

Of course, new projects rarely arise out of the blue. They typically build incrementally and pragmatically upon existing systems and processes. Hence, it is often difficult to differentiate a new system from the old, when personal information from existing applications is combined or matched to create new privacy risks.[6] Organisational decision-making is complex and iterative. Hence Flaherty remarks that a PIA is a "protean document in the sense that it is likely to continue to evolve over time with the continued development of a particular system."[7] Hence, there is a general consensus that a PIA is not just an end-product or a statement or practice. The PIA is better conceived as a *process* rather than an outcome, which is perhaps open-ended and regularised throughout the life-cycle of a programme.

Borrowing from the environmental literature, Stewart has offered the definition of a PIA as 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. An alternative definition might be that a 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."[8]

The following are some definitions and descriptions found in law, policy and guidance material from the various jurisdictions studied.

---

[1] David H. Flaherty, "Privacy Impact Assessments: An Essential Tool for Data Protection," in S. Perrin, H. Black, D.H. Flaherty and T. M. Rankin *The Personal Information Protection and Electronic Documents Act* (Toronto: Irwin Law, 2001), p. 265.
[2] Ibid., p. 272.
[3] Blair Stewart, "Privacy Impact Assessments," *Privacy Law and Policy Reporter (1996), vol. 39* at: www.austlii.edu.au/au/journals/PLPR/1996/39.html
[4] Ibid.
[5] Flaherty, *Privacy Impact Assessments*, p. 266
[6] Frank White, "The Use of Privacy Impact Assessments in Canada," *Privacy Files* (2001), vol. 4, no. 7.
[7] Flaherty, *Privacy Impact Assessments,* p. 272.
[8] Stewart, "Privacy Impact Assessments."

Canada

> PIAs “provide a framework to ensure that privacy is considered throughout the design or re-design of a programme…[and to] identify the extent to which it complies with all appropriate statutes. This is done to “mitigate privacy risks and promote fully informed policy”

Alberta

> 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.

Australia

> PIA is an “assessment of actual or potential effects on privacy, and how they can be mitigated”

New South Wales

> 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).

United States of America

> PIA is an analysis of how information in identifiable form is collected, stored, protected, shared and managed…[to] ensure that system owners and developers have consciously incorporated privacy protection throughout the entire life cycle of a system.

New Zealand

> PIA is defined as "a systematic process for evaluating a proposal in terms of its impact upon privacy".

Although there are different emphases, the following *common* elements surface. PIAs everywhere are designed to:

- conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified
- assess the impacts in terms broader than those of legal compliance
- be process rather than output oriented
- be systematic.

Organisational Type Definitions

To overcome the differences in terminology employed among the jurisdictions studied, the following terms are often used in this report to refer to types of organisations. Generally, in this report, these generic terms will be used, rather than employing the often long names or various acronyms of specific organisations.

central agency	The agency within government that has overall responsibility for privacy policy. This agency may have some regulatory responsibilities and usually has an advisory function.
privacy office	The organisational unit that has corporate responsibility for privacy within a ministry, department or other public body or organisation. This office may or may not have functional responsibility and the ability to prescribe privacy practices, or it may be a merely a centre of expertise.
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.
practitioners	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.
regulators	The central agency and the oversight body, referred to collectively.

Other Terms

Initiative	This term is used to collectively describe a number of proposed endeavours which may be subject to PIAs. It includes: projects, legislative proposals, programmes, information systems and may include modifications to these.
PIA tool	A methodology, process or template for conducting PIAs. Such tools are usually provided by privacy regulators to assist organisations and impose some sort of uniformity or minimum standard to the analysis.

Origins and History of PIAs

Internationally, information privacy law is based on some very similar assumptions and basic principles. Twenty years ago, however, the consensus about the issue extended merely to the basic requirements of a data protection, or information privacy, law. The enactment in a general statute of the fair information principles, and their enforcement and oversight through an independent oversight body, were generally regarded as both necessary and sufficient to deal with the problem.

Over the last twenty years, a number of factors have necessitated the development of a range of more specific policy instruments for the protection of privacy that might be applied within both private and public sectors. First, the move from the “databank” to the more decentralised networked information systems has provided a range of new data processing and manipulation techniques. Second, the distinction between public and private sectors has eroded as a result of outsourcing and privatisation initiatives. Third,

the staggering variety of intrusive surveillance techniques has subtly different privacy implications necessitating more finely tuned privacy solutions.

There is now a complicated "privacy tool kit" comprising different privacy-enhancing technologies and self-regulatory approaches, such as privacy seals, standards and codes of practice.[9] Many of these tools have been developed to encourage private sector compliance with data protection norms. But all have some relevance to government agencies, particularly those involved with electronic service delivery and other "e-government" applications. It is within this context of the search for different and innovative ways to encourage organisations to pursue responsible privacy practices that the idea of PIAs arose.

History of PIA Development and Diffusion

As with any policy innovation, the precise genesis of this idea is difficult to pinpoint with any accuracy. Roger Clarke identifies two intellectual precursors to the idea: environmental impact assessments and technology assessments.[10] The evolution of PIAs certainly needs to be understood in the context of larger trends in advanced industrial societies to manage "risk" and the assumption that the burden of proof for the harmlessness of a new technology, process, service or product should be placed upon the promoters, rather than society as a whole. Extrapolated to the area of privacy, this means that personal information systems should be "regarded as (relatively) dangerous until shown to be (relatively) safe, rather than the other way around."[11]

In the privacy realm, there are certainly quite early references to the desirability of conducting prospective evaluations of compliance with legal norms. Clarke identifies a number of early references, especially in policy documents in the United States and Canada, where the concept, if not the actual term was used. It also finds some early currency in Australia with respect to the cost-benefit analysis of data-matching programmes.[12] These early references, however, probably regarded PIAs as a "statement prepared as a condition precedent to approval of a project, or the debate of legislation."[13]

We should also remember that many early European regimes (particularly those in Scandinavia and France) were based upon a licensing model, whereby no personal data may be processed unless prior permission was received from the appropriate data protection authority. Flaherty's 1989 evaluation of data protection authorities documents instances where pre-decisional assessments were occasionally used in some European countries.[14] Such schemes have since been regarded as overly burdensome. But they were initially justified precisely because there would be a prospective analysis of personal information systems during the licensing process. Data protection regimes have a long history in some European countries. Where there have been more stringent and prospective licensing systems for certain personal data processing activities, the evaluation of compliance with applicable laws in advance of personal data collection and

[9] Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006).
[10] Roger Clarke, "A History of Privacy Impact Assessments" at: http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html
[11] Bennett and Raab, *The Governance of Privacy*, p. 62.
[12] Clarke, "A History of Privacy Impact Assessments"
[13] Ibid.
[14] David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989). P. 405.

processing has formed an integral part of the enforcement regime for a long time.[15] Indeed this process is now institutionalised within Article 20 of the European Directive which mandates the "prior checking" of certain especially sensitive information systems against applicable standards.

These various trends and influences seem to have converged in the mid-1990s when experts and officials in Canada, New Zealand and Australia began to think seriously about PIAs in a more systematic way as an "essential tool for data protection."[16] The idea spread quite rapidly around the policy community, even though policy tools took a while to develop.

It is often assumed that New Zealand has been the pioneer in PIA development and guidance, as a result of the influence and work of Assistant Commissioner Blair Stewart. In 1996, he published one of the earliest papers on PIAs, in the Australian journal *Privacy Law & Policy Reporter*. In 1996-97, the then Commissioner, Bruce Slane, adopted a policy of encouraging PIAs in particular circumstances. It should not be forgotten, however, that PIAs were introduced in the mid-1990s in the United States. Early PIA guidance from the Office of the Privacy Advocate in the Internal Revenue Service (IRS) dates from December 1996.[17]

Over the last ten years, PIAs have gradually spread as a result of guidance and recommendation issued by Privacy Commissioners in New Zealand, Australia, Canada and Hong Kong (see below). The accompanying case analyses review these histories and requirements in more detail. In the United States, which does not have a federal privacy oversight agency, PIAs have been instituted as a result of the 2002 *E-Government* legislation. In each of these countries, the relevant laws are described as "privacy" rather than "data protection" statutes. Even though many of the requirements of Canadian, Australian, US and New Zealand law are strikingly similar to the "data protection" statutes prevalent in Europe, the title does have a symbolic importance and cultural meaning that perhaps makes the notion of a *privacy* impact assessment more meaningful than in other countries.

It is also worth noting that most of the Commissioners in these jurisdictions, with the exception of those in the Canadian provinces of BC and Alberta, have advisory, rather than regulatory, powers. As Stewart notes with respect to New Zealand, "privacy impact assessments might help to marry the discretion allowed under the Act with a degree of accountability to the public where significant erosion will be caused by the actions of an agency or government."[18] Privacy protection regimes in these countries rely upon a significant level of self–regulation on the part of data users. PIAs have become one of the instruments in the toolbox of the privacy commissioner who has to rely on persuasion rather than power.

The Rationale for PIAs

Over the years, there have been many different arguments advanced in favour of PIAs. Descriptions of the benefits of conducting PIAs are common features of the guidance material produced by various regulators around the world.

[15] See, Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).
[16] Flaherty, "Privacy Impact Assessments."
[17] http://www.cio.gov/Documents/pia_for_it_irs_model.pdf
[18] Stewart, "Privacy Impact Assessments."

Here are some examples:

The guidance material in New Zealand is particularly fulsome in its discussion of the rationale for and benefits of PIAs.[19]

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";

"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" (p. 6);

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".

In Alberta it is argued that PIAs[20]:

- avoid adverse publicity, loss of credibility or public confidence and costs associated with legal or remedial actions.
- allow organisations to make informed decisions and implement mitigating measures to minimize potential impacts;

[19] Privacy Commissioner of New Zealand, *Privacy Impact Assessment Handbook, at:* http://www.privacy.org.nz/filestore/docfiles/48638065.pdf

[20] Based on a rationale for PIAs in the *Privacy Impact Assessment Primer*, Alberta Employment, Immigration and Industry, January 2007

The Ontario Information and Privacy Commissioner's guidelines for PIAs for health information organisations describe the benefits of PIAs as[21]:

- 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.

One of the only European countries to contemplate PIAs is Finland. There is no official policy in Finland yet. But the Finnish data protection authority has been advancing arguments about their potential:[22]

- To demonstrate to the public the agency's or company's commitment to privacy
- To develop better policy
- Increase transparency

Traditional Goals of a PIA

- Increase institutional compliance with data protection
- To prevent function creep
- Develop an institutional culture of data protection

In summary, it is instructive that PIAs are generally regarded as more beneficial to organisations, than to individuals. The overall goal of protecting and advancing privacy rights is overwhelmed by the obvious need to convince agencies and businesses that they are the right thing to do for other reasons: to demonstrate legal compliance, to allow organisations to develop better policy, to save money, to develop a culture of privacy

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

[22] From Data Protection Ombudsman of Finland, Privacy Impact Assessment presentation, August, 2007, pg. 15

protection, to prevent adverse publicity, and to mitigate risks in advance or resource allocation.

It is also apparent that PIAs are regarded and justified in quite broad terms to help organisations, to benefit society generally and to protect individual privacy. They also contribute to the “ounce of prevention” reasoning that has been part of the rhetoric of privacy protection oversight agencies for a long time. PIAs contribute to compliance which hopefully reduce the numbers of complaints, and alleviate the need for subsequent investigation and audit.

The breadth of purpose, however, also has implications for the appropriate methodology. These goals suggest that organisations should not only look at internal processes, but at a number of external impacts. While there is some common agreement on the value of PIAs, and the reasons why they are a good idea, there are, however, some variations in the ways they have been implemented in the different jurisdictions under study.

II. FINDINGS

The appended Jurisdiction reports indicate that PIA processes vary along ten interrelated dimensions:

1. Level of prescription (whether the conduct of PIAs is discretionary or required)
2. Application (type of organisation that is expected to conduct PIAs)
3. Conditions (what type of initiative or circumstances trigger a PIA)
4. Breadth of Instrument (type or comprehensiveness of the analysis)
5. Who completes them (programme, privacy staff or others?)
6. Timing (when the PIA is conducted and if it is a snapshot or multi-staged)
7. Process of Review / Approval (are they reviewed externally, by whom, and to what end?)
8. External Consultation (with outside stakeholders)
9. Transparency (whether and how reports are made public)
10. Reviews of PIA Processes

1. Levels of Prescription

Why should organisations conduct PIAs? The conduct of PIAs may be required by legislation, prescribed by binding policy, or recommended by those with no direct authority over the organisations whose operations might be subject to PIAs. The landscape can be very complex. In some cases, all three levels of prescription exist within a jurisdiction with regard to different types of organisations and initiatives. For instance, the higher level of prescription often applies to government departments or ministries, for which PIAs might be strictly required or recommended for some types of initiatives and recommended or suggested for others. Regulators might recommend that other types of public bodies conduct PIAs for some initiatives. There can also be differences in levels of prescription within jurisdictions that have separate statutes for health organisations and other public bodies.

Organisations also conduct PIAs in the absence of any level of prescription, but based on their perception of the benefits. These motivations are typically more common in private sector organisations concerned for reputation.

Legislative Mandate

In very few jurisdictions studied, are PIAs *legislatively* mandated. Exceptions are the United States of America and British Columbia. In addition, in Alberta and for a few health organisations in Ontario, the health information statutes have mandatory PIA (or PIA-like) provisions.

When PIAs are mandated, their nature is dictated by the language of the statute. The USA federal *E-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).” Incentives for the completion of PIAs are also built into the annual budget process, and federal IT security reviews.

In British Columbia, the *Freedom of Information and Protection of Privacy Act* requires government ministries to conduct PIAs for “a *new enactment, system, project or programme*”[23], 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.

In Alberta, the *Health Information Act* requires health information custodians to 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. In addition, PIAs must be conducted for data matching and certain disclosures of personally identifying health information.

In Ontario, in a Regulation under the *Personal Health Information Protection Act,* “health information network providers must 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, regarding threats, vulnerabilities and risks to the security and integrity of the personal health information; and how the services may affect the privacy of the individuals who are the subject of the information.”[24]

Experience in the US in particular suggests that the legislative mandate produces a large number of privacy impact statements. Having privacy documentation in place is a necessary condition for receiving budget approvals especially for IT procurement projects. PIAs ensure that there is some level of analysis of privacy risk within federal agencies. However their effectiveness varies depending on whether there is in-house privacy expertise. More often than not, they are compliance checks completed without a broader analysis of privacy risks. There are also some delays in completing PIAs, especially when there are insufficient staff resources.

In BC as well, the legislative mandate ensures a consideration of privacy issues within Ministries that might not happen otherwise. The greatest benefits are achieved when the PIA is conducted early enough in the process. There are also benefits with having central agency experts review the PIAs, which is required by policy. On the other hand, there is the perception that the PIA process is a net drain on resources of little benefit for the creator or the regulator, despite many instances of the PIA resulting in positive changes to initiatives.

In Australia and New Zealand, while there are no broad legislative mandates requiring PIAs, there are narrow legislative requirements requiring PIAs for Information Matching in New Zealand and Data Matching Program Protocols in Australia.

In summary, legislative mandates require a lot of work in the completion of PIAs, work that typically can only be achieved through checklists. Such forms do not require practitioners to ask the big policy questions, although accompanying guidance might suggest it.

In Australia, the Office of the Privacy Commissioner has drawn attention to the risks inherent in legislatively mandated PIAs. Organisations might focus on compliance rather than adopting a strategic approach, and might therefore fail to gain the benefits that are

[23] This requirement is in s. 69(5). Under FOIPPA s. 69(1) definitions, "privacy impact assessment" means an assessment that is conducted to determine if a new enactment, system, project or programme meets the requirements of Part 3 of this Act.
[24] under s.6(3)(5) of Ontario Regulation 329/04 of PHIPA

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 the prescriptive dictates by the legislature.

Policy Mandate

PIAs are considered 'mandated by policy' where the policy is promulgated by a regulator with the authority to issue binding direction. The regulator can be a central agency charged with that authority under privacy legislation or an organisation with authority over administration and financial management or information technology under other legislation. Policies requiring the conduct of PIAs may apply to only a subset of the organisations subject to the legislation because others are beyond the policy authority of the mandating body.

At the Canadian national government level, Treasury Board policy requires departments and agencies to conduct of PIAs for proposals for all new programmes and services that raise privacy issues. The policy applies to all government institutions listed in the Schedule to the *Privacy Act*, except the Bank of Canada. These include Departments and Ministries of State, as well as a range of government related institutions including the majority of the Crown Corporations (e.g. Canada Lands Company Limited, Canada Post Corporation, Telefilm Canada), federal agencies (e.g. Canadian Transportation Agency, Canada Revenue Agency) and other bodies funded by, or with boards wholly or partially appointed by, government (e.g. Canadian Wheat Board).

In Ontario, PIAs are required by policy at 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. The Ontario PIA process is very much seen as part of, or complimentary to, the mandated Threat Risk Assessment process, and is designed primarily to aid management decision-making processes.

In British Columbia, where the Minister has explicit legislative authority to provide direction for the conduct of PIAs, it has been used to create policy adding procedural requirements, such as review by the central agency and requiring the use of the official format and process. However, the majority of public bodies subject to the same legislation are not required to conduct PIAs and the Minister cannot direct them. These include closely-held agencies, boards and commissions, local governments and self-governing professional bodies. However, occasionally, these public bodies conduct PIAs on their own initiative, using the official process.

Recommended

PIAs are considered 'recommended' if the organisation advocating their conduct does not have the authority to issue binding direction to the target organisations or if the wording is such that the conduct of a PIA is optional.

Central agencies usually have the authority to issue binding policy, but commonly, oversight bodies are only able to exhort or recommend that organisations conduct PIAs. However, such recommendations often carry significant weight, given that a Commissioner might publicly comment if its privacy concerns are not addressed.

Regulators may recommend that a PIA be conducted when approached for advice on a specific proposed initiative. They can find that, when an organisation conducts a PIA, it makes that organisation better prepared to answer questions and respond to their

concerns, and in some cases, the exercise has already caused the organisation to consider changes to the initiative.

The Privacy Commissioner of Hong Kong has a history of suggesting that PIAs be undertaken for specific initiatives and has produced guidance that describes circumstances in which the Office recommends the completion of PIAs. However, they are not mandatory.

In Australia and New Zealand, the PIA tools are the product of the oversight bodies which have no direct policy authority. Recommendations of the Australian Commissioner in particular, but also the Victoria Commissioner, have considerable moral suasion, and many agencies have performed PIAs, or felt themselves to be under pressure to do so. The New Zealand Commissioner, in a conflict with the department of transportation, managed to convince Cabinet to issue an instruction for a PIA to be conducted. Ontario's *Personal Health Information Protection Act* does not require PIAs to be conducted by 'health information custodians' (the majority of organisation subject to the statute), but their conduct is recommended, and promoted heavily, by the oversight body.[25] The oversight body also produced a set of specialised guidelines.

2. Application – Which organisations complete PIAs?

Public Sector PIAs

In each of the jurisdictions under study, there is a longer history of regulation of the public sector than the private. In the Canada, New Zealand, Australia and the United States, public sector privacy legislation has generally predated that for the private sector. Therefore, most PIA *requirements* apply to public sector organisations such as government ministries or departments and types of public bodies or agencies.

However, it is increasingly difficult to determine the limits of the public sector under current conditions. Many other 'public' agencies outside of central government ministries now have extensive experience with PIAs. This includes: organisations in the health sector, especially where health care delivery is a public service; organisations in higher education; and statistical agencies. Increasingly, PIAs are also conducted for high-profile national identification schemes. For instance, the Hong Kong ID Card was the subject of a PIA at each of four phases between 1999-2000 and 2004.

PIAs are mostly conducted by organisations subject to privacy regulation. However PIAs could be conducted by organisations that are not subject to privacy law. They could merely modify the compliance check refer to privacy principles or standards as the yardstick, instead of the law, or they could conduct the compliance exercise as if the law applied. The types of public sector organisations required to conduct PIAs are described in the section above.

Private Sector PIAs

There are no examples, in the jurisdictions studied, of PIAs being *required* for private sector organisations, and we do not know about the extent to which private sector organisations conduct PIAs in the absence of a mandate. However, they have been recommended by privacy commissioners both generally and for high-risk situations or initiatives. In New Zealand, for example, the guidance material is explicit that the PIA

[25] In contrast, PIAs are required under subordinate legislation for a small group of organisations covered by PHIPA - 'health information network providers'.

"should be useful to any public or private sector agency that handles personal information, particularly medium to large businesses and government departments".[26] And the literature cited above is explicit that PIAs should be of equal value to the private sector as to the public.

We certainly have sufficient evidence to say that PIAs of some description are being carried out in the private sector in each of the jurisdictions we have studied. They are more likely to be carried out where, first, companies have high-profile privacy expertise in the form of Chief Privacy Officers. In Canada, for example, TELUS, a national telecommunications company whose Chief Privacy Officer is a high-profile and active participant in the privacy community, has reported on the PIAs conducted for new telecommunications initiatives. The Royal Bank of Canada also incorporates PIAs into their IT infrastructure projects at the product initiation and requirement phases, followed by audits using development and compliance checklists at the design and acceptance phases. Secondly, they will also be conducted in the context of the private sector delivery of government schemes (such as road-pricing, IT infrastructure projects, smart card applications). And thirdly, they may be carried out where corporations have been the subject of public embarrassment, for example as a result of high-profile data breaches; Hewlett-Packard in the US is an example.

However, there is really no way to determine how many and what types of organisations conduct PIAs where they are not required or reported. Unlike in the public sector, there is no comprehensive documentation available. Some of the PIA processes for business are also likely to be considered proprietary, because they can confer competitive advantage in the particular marketplaces where they are most likely to be used – e.g. telecoms, banking and private health services.

3. Conditions and Circumstances for Conduct of PIAs

What types of initiative or circumstances trigger a PIA? For what *undertakings* are PIAs carried out?

Some jurisdictions have developed screening tools to help organisations determine if they should conduct a PIA for any given initiative, or to help them identify privacy issues that may require further analysis. Commonly, a screening exercise is conducted initially to determine if a PIA should be completed according to the rules or recommendations in the jurisdiction. This can be as simple as determining whether personal information is involved, or take the form of a structured instrument that poses a series of questions (as in New Zealand.) The US Department of Homeland Security employs a form for a Privacy Threshold Analysis to determine whether a PIA is required.[27] Those completing the form provide a variety of information about the system, answering specific questions tailored to their operational context, and the privacy office makes an assessment the subject of analysis is or is not a Privacy Sensitive System.

In the government of Canada, a multi-staged assessment is formalised in policy. The process includes a Preliminary PIA and the full PIA later. The Preliminary PIA (PPIA) will not be as comprehensive as the PIA but will serve to indicate to departmental

[26] Privacy Commissioner of New Zealand, *Privacy Impact Assessment Handbook, at:* http://www.privacy.org.nz/filestore/docfiles/48638065.pdf

[27] Department of Homeland Security, Privacy Threshold Analysis, July 2007, at: http://www.dhs.gov/xlibrary/assets/privacy/DHS_PTA_Template.pdf

programme managers whether or not there are significant privacy risks for a proposal.[28] The PPIA is a bit like a screening tool, but is also a short-form PIA, similar to a Privacy Scan or Privacy Impact Statement in other jurisdictions.

In some cases, PIAs are only required for new initiatives, although it is more common that they also be carried out for changes when they have privacy implications. For example under the 2002 E-Government Act in the US, PIAs are conducted when organisations are developing or procuring *information technology* or initiating *any new collections of personally-identifiable information*.

Research did not uncover a jurisdiction which provided a different PIA process for different types of initiatives, although there are some portions of a template that can only be completed for certain types of projects (e.g., information system security). However, the reported direction of the British Columbia review and revision project is that it will tailor PIAs for legislative proposals, information systems, other projects and incremental changes to existing programmes or systems.

New Zealand's PIA guidance material provides a fairly complete answer to the question, "What factors are seen as determining which projects need PIAs?"[29] More specifically, project characteristics that indicate the need for a PIA include:

- 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

In the US, the guidance from the Office of Management and Budget suggests the following conditions[30]:

- 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

[28] *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
[29] Privacy Commissioner of New Zealand, *Privacy Impact Assessment Handbook, at:* http://www.privacy.org.nz/filestore/docfiles/48638065.pdf
[30] OMB, E-Government Act Section 208 Implementation Guidance, http://www.whitehouse.gov/omb/memoranda/m03-22.html

- 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
- 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)

It is clear that there can be no exhaustive list of conditions that should always motivate a PIA exercise. The potential for risk is going to be dictated by the nature of the initiative, and the context within which it is introduced. There can be no automatic "triggers" which can replace the exercise of human judgment.

4. Breadth of the PIA Exercise

By breadth of the PIA exercise, we mean the comprehensiveness of the analysis. There is a general consensus, as Flaherty remarks that organisations "must prepare privacy-impact assessments in such a manner as to identify key problems, not gloss over, or skip by, them because the specialists in the offices of privacy commissioners will focus on them in the long term."[31]

Generally, where PIAs are prescribed or recommended, either the central agency or the oversight body provides a process guide and/or a template for presenting the results of the analysis. Not only do the processes outlined vary widely in their comprehensiveness, but the quality and quantity of guidance varies as well. The majority of templates are either questionnaires organised along the lines of the data protection legislation, or report outlines indicating what types of information should be covered under various headings. Generally, PIA templates are available both as paper documents and in electronic format which may be completed electronically.

Process guides tend to be more comprehensive and suggest the various stages of the PIA process. An illustration is within the guidance provided by the Australian Privacy Commissioner, which has described five key stages[32]:

- Project description: broadly describe the project, including the project's aims and whether any personal information will be handled;
- Mapping the information flows: describe and map the flows of personal information in the project;
- Privacy impact analysis: identify and analyse how the project impacts upon privacy;

[31] Flaherty, "Privacy Impact Assessments," p. 268.
[32] http://www.privacy.gov.au/publications/pia06/index.html#mozTocId799546

- Privacy management: consider alternative options, particularly those which will improve privacy outcomes whilst still achieving the project's goals;
- Recommendations: produce a final PIA Report, which includes the above information and recommendations.

An integral part of most PIAs is an analysis of the flows of personal information. The Australian guidance goes on:

> Once a broad description of the nature and scope of the project has been completed, the next stage in a PIA is to describe and map the flows of personal information in the project. This could include:
>
> - what personal information is to be handled in the project;
> - how the personal information is to be collected;
> - how it will be used;
> - internal flows;
> - disclosures;
> - security measures; and
> - any privacy, secrecy and other relevant legislation applying to those flows.
>
> In order to effectively map the information flows, communicating with all relevant sections of the agency will be important. Attempting to complete this stage in isolation runs the risk that valuable information about how the project will work, and how any personal information will be handled, may not be taken into account. This could lead to difficulties as the project develops.
>
> This stage of the PIA should also describe the environment that currently exists, and how the project will affect this environment. For example, where a project involves new uses for personal information already held by an agency, this description could identify the nature of such personal information and the context in which it was initially collected (including the purpose of collection). Illustrating the data flows using diagrams or maps can give a clearer picture.

Similar advice is provided within the Privacy Impact Assessment Guidelines within Ontario. The process of conceptual analysis, data flow analysis and follow-up analysis is depicted in the following table.

Ontario 3-stage PIA process[33]

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	Analyse 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 programme 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 analyse 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 programme statutes, and broader conformity with general privacy principles Prepare a communications plan

It was generally found that this kind of guidance is useful to the organisation and the regulator. If this analysis is conducted well, then it is readily accessible to departmental users in the future and may be built into future PIAs as the system/programme/technology matures.

These flow analyses also point up the distinction made earlier between process-oriented and product-oriented PIAs. The latter is exemplified by the PIA policies in the USA where the legislative mandate requires the production of privacy documentation, which is now also a condition for receiving budget approval, especially for IT procurement. There is evidence that OMB will sometimes send the PIA report back to the agency if it is not sufficiently comprehensive. Product-oriented PIAs do improve transparency, where none might have existed before. But they may also be based on a very cursory or superficial assessment exercise. Furthermore, the form and length of the output may disguise the extent of the analysis conducted. For example, one might see a very lengthy report which might be based on a quite superficial process. Conversely, there might be a brief report which shields a quite comprehensive analysis of the personal data flows, and the risks.

A comprehensive PIA should also be open-ended, far more than merely compliance-focused, and serial, as in cumulative experience along the project life-cycle. It would include consideration of a variety of aspects of privacy and would be as broad or narrow as the issues posed by a particular initiative dictated. 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

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

imposition of biometric measurements), privacy of personal behaviour (e.g. visual surveillance) and privacy of personal communications.

The proposed Finnish model, currently under development, proposes consideration of some factors not currently found in PIAs. An example is the consideration of cost-effectiveness, including practicality and suitability. It also takes a human rights approach which considers data protection and basic rights as well as justice and ethics, and looks for innovation and value-added.[34] It is not yet clear how these concepts will be translated to the Finnish PIA tool.

5. Who conducts PIAs?

Almost universally, programme or business areas have responsibility for producing the PIA but draw on a variety of expertise. PIAs are usually completed at the senior analyst level or by a manager with ongoing programme administration responsibilities. Less often, PIAs are conducted by the organisation's privacy office with information provided by programme staff, but this decision is not so much jurisdictions-specific as organisation-specific. In no cases, did we find PIAs being conducted by the oversight office itself. Oversight agencies do not have the resources and do not necessarily possess the relevant technical and programme knowledge. Furthermore, many initiatives will not be public knowledge at the point where the PIA is going to be most useful.

Guidance material often suggests a team or committee approach and stipulates what types of expertise should be drawn in to the PIA. This can include, with varying degrees of participation:

- Programme and project managers
- privacy policy advisors
- legal advisors
- records management staff
- information technology or data security experts
- communications staff
- legal officers
- other functional specialists, as appropriate

Organisations conducting PIAs often "consult" internally to government, with other agencies who may or may not be involved with the initiative, and project contractors.

New Zealand's guidance discusses team formation in terms of skills required, and includes many of the above plus: policy development (broad strategic policy and planning and consultation), operational programme and business design, risk and compliance analysis skills.[35]

[34] Data Protection Ombudsman of Finland, draft Privacy Impact Assessment presentation, August, 2007, slide 23, *3 Part Test*.
[35] Privacy Commissioner of New Zealand, Privacy Impact Assessment Handbook, at 5. Who Should Undertake Privacy Impact Assessment at: http://www.privacy.org.nz/library/privacy-impact-assessment-handbook

The Role of Consultants

A trend, particularly seen with information systems initiatives, is to have consultants conduct or play a role in the completion of the PIA. This requirement is often seen in procurement documents. While in some jurisdictions, the consultant plays a major role and is seen as conferring independence and credibility, in others, the consultants were seen as a useful part of a PIA team, bringing their particular expertise to a process run in-house.

In Hong Kong, the limited PIA guidance material suggests 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. 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."[36]

In Alberta, where a very large number of health service delivery organisations of all sizes are subject to legislation requiring PIAs, expertise in conducting PIAs has been gained by information system vendors. These vendors offer their services in conducting PIAs as a service sold with the system. This is particularly helpful for small organisations that have no privacy and small administrative staff.

In New Zealand, the oversight office observed that there were only a limited number of people with the expertise to conduct PIAs or to advise on their planning and conduct. Therefore, it is 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.

The Privacy Commissioner of New South Wales (Privacy NSW) in his June 2004 Submission to a Review of the Privacy and Personal Information Protection Act, recommended that PIAs be completed by an independent party like a consultant or the Commission. However, as the latter is short on resources, he proposed a model whereby the cost would be borne by the organisation whose initiative is under assessment, and would entail:

- Privacy NSW to help setting terms of reference for a PIA, including what external guidelines / standards to use; and
- PIAs being conducted by an independent consultant, who reports to Privacy NSW as well as the client

The Privacy Commissioner of Victoria intends, in her next revision of the PIA guidance, to advocate organisations 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.

Consultants can also play the role of providing frank advice when initiatives are simply unwise or ill-conceived. There are examples, especially in Australia and Canada, where expert consultants have been able to divert a project at a very early stage, not only for

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

privacy reasons, but because they are also able to ask some of the more penetrating questions about cost-effectiveness and programmatic goal attainment. In some instances, further PIAs are unnecessary because the project has been dropped completely.

When consultants have considerable experience in a particular niche, they often have greater expertise and familiarity with privacy laws, relevant technology, and previous privacy breaches than programme staff. However, there is a danger that consultants are not attuned to social mores and public opinion on privacy issues when they work in new public policy fields. In addition, their cost may be prohibitive for smaller organisations and initiatives. The use of consultants may also undermine attempts to build internal privacy awareness and expertise. There is also some scepticism about the 'cookie-cutter' PIAs where consultants mould the process to fit their own templates and methodologies at the expense of capturing the nuances of particular projects or particular departments. However the role of the consultant need not be to carry out the PIA alone, but to add a degree of objectivity to an in-house process as part of a committee of people drawn primarily from the department.

6. Timing of Conduct of PIAs

PIA tools are designed to be applied to initiatives under development, at a time when the personal information aspects are known, but before decisions are set in stone and become very expensive to change. Guidance material often stresses the importance of conducting the PIA early enough so that results of the assessment can have the opportunity to influence the developmental process of the initiative.

Of course, projects and services have complicated histories, and it is often difficult to define them in terms of a clear beginning, middle and end. Most of the better guidance is sensitive to these realities.

For example, the approach in Ontario is intended to be carried out iteratively from the conception of the project to the point of implementation. Guidance material states that "the PIA is best approached as an evolving document, which will grow increasingly detailed over time."[37] As noted above, the Ontario PIA User's Guide divides the PIA process into the three stages: conceptual analysis, data flow analysis and follow-up analysis. It includes a set of charts for undertaking a data flow analysis, which aim to generate comprehensive documentation of data flows through business processes, identify specific personal data elements or clusters of data, and identify potential privacy risks that will require solutions.

In the Canadian federal government, it is noted that "the assessment process is iterative, meaning that it is to be updated, maintained, re-designed or altered throughout the life cycle of a programme or service."[38]

The process stipulated for PIAs for implementation of new health information systems receiving department of health funding in Alberta requires a 6-month post-implementation audit to ensure that mitigation measures have been implemented.

[37] Ontario, *Privacy Impact Assessment Guidelines*, p.11.
[38] Government of Canada, Treasury Board Secretariat, *PIA e-learning tool*, October, 2003, at: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a_e.asp

7. Process of Review / Approval

PIAs are generally subject only to internal agency review and approval processes, and these are generally not prescribed, but at the discretion of the organisation. However, accountability for the conduct of PIAs is achieved in part by having PIA reports submitted to and reviewed by a privacy regulator.

Jurisdictions where PIAs are reviewed externally are:

- British Columbia, where the central agency reviews and 'accepts' PIA reports,
- Ontario, where the central agency reviews reports,
- Alberta, where the oversight body reviews and 'accepts' PIA reports and
- Canada, where the oversight body reviews, but does not accept or reject them.

In British Columbia, the review of PIAs is not mandated for all types of initiatives or for all public bodies conducting PIAs. Almost all PIAs are eventually given an acceptance letter unless the initiative is withdrawn, and that is usually not due to reasons relating to privacy.

In Ontario, the Ministry of Government Services uses the PIA process and the resulting reports to ensure that project privacy risks are adequately documented, assessed and addressed. The process is designed to support senior management decision making – should this project be funded – in the event that management is not convinced by a report the project is less likely to be funded at that point. The aim is that projects will complete a draft PIA early in the development process, well in advance of submission date to Management Board (MB) and then MGS staff will review the draft and work with projects to get the PIA Report to a point where MB can make a decision on the project relatively quickly. This does not always occur, and sometimes lengthy discussion may take place in front of MB.

In reviewing PIA reports, the Alberta Office of the Information and Privacy Commissioner sees no conflict between the roles of PIA reviewer and the order-making and investigative powers of the office. The overview material makes it clear that acceptance is not approval, and that PIA review does not prevent future investigations or findings against the organisation regarding the subject of the PIA. The office is careful not to recommend the measures by which privacy issues identified should be addressed.

The Information Privacy Commissioner of Alberta's message in his 2005/6 Annual report[39] groups his office's review of PIAs with "requests for information and comments on programmes and schemes". Together, he thinks this "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."

In the national government of Canada, PIAs are reviewed by the audit and compliance staff of the Office of the Privacy Commissioner of Canada, which does not approve or reject, but comments on the quality of the process undertaken.

In the United States, the Office of Management and Budget (OMB) Guidance specifies that agencies must also ensure that the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency Chief Information Officer or other agency

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

head designee, who is other than the official procuring the system or the official who conducts the PIA). Some agencies, such as the Department of Homeland Security, have separate privacy protection offices which play this role. OMB is the major central budget coordination agency within the federal government. Thus, incentives for the preparation of PIAs are also built into the annual budget approval cycle. Agencies must have privacy compliance documentation in place before going to OMB for funding. 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.

In Hong Kong, the oversight body may provide critique and feedback on PIA reports, but does not play any role such as formal advisor, consultant or inspector.

In Australia, Victoria's Privacy Commissioner has announced her intention to revise her PIA guidance, including clarification of her office's role as a discussant and reviewer of PIA outcomes, but not as a formal 'approver' of PIA processes or reports.

Where PIAs are reviewed by a regulator, there is usually a process of communication between reviewer and agency representatives. The reviewer often seeks clarification or further information, raises concerns and discusses alternatives, although the PIA sponsor makes decisions about how to address issues. Communication can take the form of meetings, formal correspondence, or informal telephone calls and electronic mail. Where PIAs are accepted, it is more common to have this communication take place than have a report accepted 'as is'.

Changes are frequently made during the review process, and the regulators involved in PIA reviews commonly feel that they contribute value. Reviewers may be aware of what can go wrong with initiatives of the type proposed or be aware of public sentiment regarding personal information practices. Reviewers may inform the PIA sponsor of alternatives and technology that could be less privacy invasive, but not go as far as telling the organisation what choice to make. PIA sponsors are usually very receptive to input and seldom resist addressing reviewer concerns.

For example, 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, a full credit, Canadian Security Intelligence Service (CSIS) and criminal record check 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.

An unintended benefit of having PIAs reviewed is that initiatives from the far corners of government can benefit from a corporate perspective, sometimes unrelated to privacy or matters of privacy compliance. Central agencies, with their corporate perspective, are able to draw the PIA sponsor's attention to competing or complimentary initiatives or government direction, in addition to addressing privacy issues from a broader knowledge base than practitioners.

8. External Consultation

Consulting with outside stakeholders, and particularly those constituencies who are directly affected by a proposal, can provide deeper insights into an initiative's likely negative impacts, and suggest what can be done to avoid or ameliorate them. In extreme cases, advance warning could be gained of serious public sensitivities.

Some jurisdictions' PIA methodology suggests that public or stakeholder consultation be conducted during the PIA. The Australian Privacy Commissioner's Guidelines state: "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".[40] Some innovative consultation practices have been used in Australia. They include forming a PIA consultative group of representatives of people in various client segments, together with advocates for consumer and privacy interests.[41] Confidence in the consultation process is enhanced when stakeholders see their input having been incorporated in later rounds of consultation.

Ontario's PIA user guidelines argue that: "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."[42] Despite this, the extent to which public consultation, as opposed to external project stakeholder consultation (regulators, other agencies, third party vendors and service providers) takes place in many departments/agencies appears limited. In Alberta, PIA guidance goes further, stating that "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."[43]

Even if external consultation is required or suggested, guidance is scarce, and in practice, external consultation is rare, although it may be conducted with regard to the initiative in general, rather than its privacy aspects. This reality is probably explained by the nature of the process in which the PIA is embedded. In all jurisdictions it is predominantly seen as a way to facilitate senior management decision-making.

The importance of consultation with outside stakeholders is highlighted by some of the experience in the United States. The Department of Homeland Security is responsible for some of the most intrusive and controversial initiatives associated with the War on Terror. It also has an institutionalised Privacy Office and considerable experience with PIAs. However, some of these initiatives are subjected to an extraordinary amount of commentary and criticism from the media and the non-governmental organisation community after they have been announced and after the PIA is published. Privacy advocates tend to believe that risks can be averted, and money saved, if there were a higher level of external consultation during the PIA process.

[40] Australian Privacy Commissioner, *PIA Guidelines*, p. 9 at: http://www.privacy.gov.au/publications/pia06/index.html#mozTocId799546

[41] These methods were employed by Centrelink, the delivery channel for about 100 benefits programmes run by various Australian government agencies.

[42] Ontario, *Privacy Impact Assessment A User's Guide* (2001) Access & Privacy Office, Ministry of Government Services, p.27,at: http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf

[43] Service Alberta, PIA Guidance and Practices at http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3

9. Transparency

Public Availability of PIA Reports

Practices vary with respect to the public availability of the PIA reports. The US E-Government Act requires agencies to publish PIAs "to the extent practicable". Most PIAs are published in the United States and even available on-line. Requests for non-public reports are dealt with under the freedom of information legislation and procedures including redacting.

Australian privacy commissioners are on record advocating publication of PIA reports and the federal government's guidance material envisions this. The Federal Privacy Commissioner has recommended that: "Privacy legislation should make it mandatory for all Commonwealth agencies and private organisations to provide and publish Privacy Impact Assessments (PIAs) for all new programmes, policies and draft legislation which impacts on the handling of 'personal information'. The PIA provides for accountability and greater transparency in decision-making." The NSW Commissioner, in his June 2004 Submission to a Review of the Privacy and Personal Information Protection Act 1998 stated that "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."[44]

Canadian government departments and agencies are required to make summaries of the results of their PIAs available to the public. These may be redacted to remove information excepted from release under freedom of information legislation and which would render systems or security measures vulnerable. Publication has to be in a timely manner, using plain language, in each of the two official languages, and consideration should be given to regular and internet publishing. In practice, departments fall short by failing to publish and in the quality of information.

In Canada's provinces, where PIA reports are not required to be made public, they are made available to the public on request under freedom of information legislation, and may be subject to severing.[45] This process entails waits of up to and more than the statutory time limits to receive reports and may involve the payment of application and duplication fees.

There is, however, an inherent dilemma. If PIAs are to be considered "pre-decisional" tools then they would generally not be expected to be published, and would not be accessible under most national FOI legislation. In most jurisdictions, the requirement that PIAs are pre-decisional invariably means that there is no publication until they are complete, reviewed by counsel and signed off by the relevant agency official.

Directories of PIAs Conducted

Public directories listing the PIAs conducted are a means by which some jurisdictions make known what PIAs have been conducted. Without these, it would be difficult for interested parties to determine whether an initiative is being implemented and if a PIA has been conducted, unless the initiative were high-profile and had received media attention or was subject to general (not privacy-related) consultation. In Canada, the

[44] Privacy NSW, Submission to a Review of the Privacy and Personal Information Protection Act 1998, June 2004, at: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_ppipareview.doc/$file/sub_ppipareview.doc

[45] One of the authors has recently received through Canadian Access to Information legislation, a redacted version of the PIA conducted for the Canadian no-fly list program, "Passenger Protect."

provinces of British Columbia and Alberta maintain on-line public directories. These list the initiative by sponsoring organisation and contain a brief description of the initiative, but do not summarise the PIA.

10. Reviews of PIA processes and instruments

Various types of reviews of PIA tools and processes are fairly common. This is not surprising, given the pressures on privacy protection posed by increased digitisation of personal information and the global security situation. Tools for assessing and mitigating privacy risks become even more important under such pressures.

The Canadian jurisdictions surveyed had all amended their PIA processes since initial development, although changes have not generally been fundamental. Currently a fairly ambitious review and revision exercise is underway in British Columbia and at the federal level in Canada. Australia's 2006 tool has not yet been revised but the Commissioner's Office is looking to review and enhance the guide in 2008. There is also a rich history of comment during legislative reviews regarding PIAs, including a recommendation by the Australian Commissioner that PIAs should be legislatively mandated.

A study was recently completed for the Ontario government[46] which included an audit of PIAs in the area of Shared Services. The 2005 report provided clear evidence of lack of compliance with policy, and quality issues, including incomplete and untimely reports, failure to identify privacy issues at an early stage and, in some cases, no PIAs being carried out. Recommendations were made for improvements to the process. However, 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.

The Ontario review reflects two increasing trends amongst regulators. Firstly, 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". Secondly, 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.

New PIA development projects underway

Finland is developing a PIA tool which is likely to take the form of a questionnaire. At an early draft stage, it seems to focus on new data processing systems and has some unusual sections relating to human rights, sophistication of the user and sensitivity of data.

The NSW Commissioner, in his June 2004 Submission to a Review of the Privacy and Personal Information Protection Act 1998 advocated for PIAs to be introduced by the government. More recently, the Privacy Commissioner of New South Wales expressed a desire to develop a guide to PIAs in the near future.

In Australia, the Victoria Privacy Commissioner has stated her intention to review the PIA Guidelines in the near future, with the expectation that key messages will be strengthened

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

and clarified, and a review of the national Commissioner's guidance material is slated for 2008.

Studies underway

In British Columbia, the central agency is nearing completion of a major review and revision of the PIA template which involved consultation with PIA users.

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.

III. LESSONS FROM INTERNATIONAL COMPARISON

The case studies suggest the following international trends, as well as some lessons for the most effective conduct and completion of PIAs.

Trends

1. Spread of use of PIAs

The most notable trend is the spread of PIAs across jurisdictions with privacy regulation in a similar manner as privacy regulation itself has spread. PIAs have been spreading around the advanced industrial world as a result of: legislative requirements; policy guidance by central government agencies; recommendations by privacy and data protection commissioners; and recognition by organisations that PIAs can expose and mitigate privacy risks, avoid adverse publicity, save money, develop an organisational culture sensitive to privacy, build trust and assist with legal compliance. While this spread has not been universal, there is a common consensus that PIAs are a good idea. That view is increasingly recognised as such by privacy commissioners, government agencies, private corporations and privacy advocates.

2. Spread from public to private sectors

Although requirements or recommendations for private sector organisation to conduct PIAs is less common outside of Europe, regulators familiar with the process occasionally recommend their conduct to organisations that consult them and even advocate their use generally in the private sector, despite lack of mandate.

In addition, when those responsible for privacy within private sector organisations attend conferences and follow developments in the privacy community, they learn of the existence of this tool and have been known to apply it in their organisations on their own initiative where they feel it is warranted. Consultants also have some responsibility for the spread between sectors.

3. Improved Compliance

'Compliance' is used in the sense of the degree to which organisations follow the legislation, policy, guidelines and recommendations regarding PIAs in place in their jurisdictions.

The early experience has been evaluated in several jurisdictions, and lessons are being drawn about the most effective way to encourage their effective completion. Generally, incomplete compliance was found regarding the incidence of PIAs being completed when they were mandated or recommended. Completeness and quality of analysis (within the process prescribed in the jurisdiction) has also been a little sub-standard, as evidenced by the fact that so few PIAs are accepted immediately where they are externally reviewed.

Some of the deficiencies found by those reviewing PIAs include:

- reports are incomplete, missing a required attachment or section, or answers to specific questions in the PIA instrument
- descriptions are at too high a level to fully understand what is proposed
- organisations have failed to realise the highly sensitive nature of the personal information involved in their initiative and failed to take appropriate measures

- organisations propose collecting more personal information than is strictly necessary for the achievement of programme goals, or are mistaken about their authority to collect it
- organisations identify a privacy risk, but fail to provide an action plan to demonstrate how it intends to address that risk

However, there is evidence in many countries that compliance and quality are improving over time, as guidance materials are amended and proliferate and experience conducting PIAs increases and spreads.

Compliance is also enhanced when PIAs are integrated into existing management processes such as those for project approval and funding, project management, IT procurement or quality assurance.

Several authors have suggested that organisations can benefit from adopting a comprehensive approach to privacy, linked to overall corporate strategy. By ensuring that staff at all levels are well aware of privacy, and take it into account when they are dealing with customers, privacy issues will be identified earlier, and PIAs will be much easier and more widely performed.

4. The Scope of Analysis

There is conflicting evidence about the scope of analysis. Some jurisdictions started quite narrowly with tools barely distinguishable from a Compliance Check. In some jurisdictions there is a trend toward the maturing of the process by moving away from simple YES/NO checklists towards “telling the story” of the system technology or programme being reviewed. In some jurisdictions, there are efforts to ask the broader policy questions. In others, however, there are signs of swings in the other direction with attempts to reduce the process to routinised checklists which trivialises PIAs, and prevents genuine organisational benefits from being achieved. It is commonly viewed that simple compliance checklists are not useful in achieving the management information/ decision making support goals they were seeking to obtain.

5. Increasing Sophistication of Guidance Material

In most jurisdictions where law or policy require or highly recommend that PIAs be conducted, an official PIA template, format or other tool to describe how they should be conducted, is provided. These tend to be more useful when they are process oriented and designed to capture the dynamic information environment within and between organisations. A mechanical “checklist” alone does not capture the broader social, political and ethical implications of many initiatives.

As a jurisdiction’s experience with PIAs increases, it tends to revise and add to its guidance material. They are informed by tools used in other jurisdictions. More jurisdictions plan to introduce guides and some are in the process of expanding their guidance material.

Conditions for the Effective Use of PIAs

It can be concluded that PIAs are generally perceived to be more effective when:

1. They office a prospective identification of privacy risks *before* systems and programmes are put in place. In every jurisdiction, PIA processes have been designed to be prospective.

2. They assess the proposed initiatives within a framework which takes into account the broader set of community values and expectations about privacy.
3. When they refer to an entire process of assessment of privacy risks rather than a statement or end-product. Often, the final report or statement, if indeed published, offers a deceptive impression of the nature, scope and depth of the assessment exercise. A simple report does not necessarily indicate a simple assessment. A detailed report does not necessarily reflect a detailed assessment. Reports also do not necessarily reveal the changes made to the initiative during the PIA process.
4. When they have, and are perceived to have, the potential to alter proposed initiatives in order to mitigate privacy risks. Where they are conducted in a mechanical fashion for the purposes of satisfying a bureaucratic or legislative requirement, they are often regarded as exercises in legitimation rather than in risk assessment.
5. When their scope and depth is sensitive to a number of crucial variables: the size of the organisation; the sensitivity of the personal data; the forms of risk; the intrusiveness of the technology. A PIA screening process is commonly used to determine whether a PIA is required, and if so, the form it should take.
6. When they are part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes, as is common with other forms of threat/risk assessment. Incentives are created when project approval and/or funding is tied to the conduct of a PIA.
7. When the individuals charged with completing PIAs not only have good programme knowledge, but also have access to multidisciplinary expertise from a variety of perspectives -- privacy law and practice, information security, records management, and other functional specialists as appropriate.
8. When the PIA tool is accessible, readily available and easy to access, and the process involved is flexible.
9. When there is a process of formal or informal external review either by central agencies or privacy oversight bodies. This review may but does not need to include ‘acceptance’ or approval.
10. When there is a strong advocacy role played by the relevant oversight body.
11. When there is external consultation with outsiders affected by the initiative. Most PIA guidance suggests that key project stakeholders should be consulted, including regulators, other agencies, third party vendors and service providers, and others directly affected by the project reviewed. Public consultation is often advised. The form public consultation takes usually varies according to the scope and privacy intrusiveness of the project.
12. When there is transparency, and the resulting statements or reports are published. Openness of process and output enhances trust in the initiative being proposed.

IV. PRIVACY IMPACT ASSESSMENTS IN THE UNITED KINGDOM

Given these trends and lessons, what advice can be provided for the prospective conduct of PIAs in the UK? Not all the issues studied and commented on are factors that the United Kingdom Information Commissioner can address, at least in the short term. The Commissioner's office is not in a position to legislate or otherwise mandate the conduct of PIAs. Therefore the PIA process it advocates must be perceived as having benefits to data controllers commensurate with available resources. The PIA process itself should be one that practitioners believe is of value to their organisations and that the payback will be commensurate with the resources expended in their conduct. The ICO may not be able to provide tangible incentives, but the Office can be a strong advocate and offer support in the form of tools, training and advice. Any guidance material it produces can address the comprehensiveness and approach to analysis, the types of organisations that should conduct PIAs, the process for quality control and review and the processes used for accountability. Care should also be taken to find a way to play this role without harming the perception of its ability to perform an oversightg or investigatory role with regard to the subject of those PIAs in future.

The ICO, through its request for this international study and development of a handbook has signalled its intention to advocate for PIAs. The ICO already produces a number of guides to organisations trying to meet their data protection obligations.[47] However, in other jurisdictions, regulatory roles are played by central government agencies, and presumably the same would be the case in the UK. However, it is not clear whether the appropriate central agency would be the Ministry of Justice, the Cabinet Office or the Office of Government Commerce through its Gateway Review Process (see below).

Establishing PIA processes is not an overnight matter, and neither is the development of appropriate expertise. It has taken some jurisdictions 5-10 years to get where they are, and many of those regulators see room for improvement. However, the ICO has the potential to learn from the experiences elsewhere, and especially from those jurisdictions with equivalent oversight agencies which have attempted to encourage PIA through powers of moral suasion rather than through legislative or bureaucratic fiat. A structured and timetabled roll-out should be aimed for, and attention should be given to developing expertise in the conduct of PIAs. Over time and with experience, organisations are likely to develop internal expertise and will need to rely on the support of the ICO less. As experience grows, organisations will learn of the benefits from one another.

With these international lessons in mind, there appear certain advantages within the UK context which suggest that PIAs can be integrated into the organisational culture of British organisations, in ways that we are beginning to see in other countries. These are conditions related to:

1. Existing privacy regulations
2. Existing in-house privacy expertise
3. Incentives within existing management processes
4. External expertise in consultancy and training

1. Existing privacy regulation

Privacy or data protection regulations create the standards against which the minimum form of the PIA, the compliance exercise may be measured, and their existence can be

[47] ICO, *Tools and Resources* web page at http://www.ico.gov.uk/tools_and_resources.aspx

taken as a sign that the society at large values privacy. The UK is in a position to capitalise on its 23 year history of data protection regulation. There are strong networks of knowledgeable data protection officers, and regular opportunities for cross-organisational learning. There is also a long history of developing codes of practice within certain sectors through umbrella groups. These groups, if brought on-side, could be very useful in the introduction and spread of PIAs.

At the European level, Article 20 of the EU Data Protection Directive on "prior checking" should be kept in mind:

> "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."

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. 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. To date, however, no order has been yet been made in the UK.

The prior checking requirement is directed towards some precise categories of data, and therefore, where implemented, tends to lead to legislative compliance checks which are narrower than our conception of PIAs. But European practice varies considerably, and there is evidence (cited in the Jurisdiction Report on the EU) that some jurisdictions (for example in Germany) are interpreting this requirement more broadly than others. In the European context, PIAs might be regarded as an extension and expansion of Article 20 requirements. In the UK, although the preliminary assessment process is not used, it is on the statute books and may be relied upon, at least for certain forms of processing, to justify PIAs.

2. Existing in-house privacy expertise

Every PIA should involve interplay between privacy and programme experts. Even though most jurisdictions require the PIA to be completed largely by programme or business area staff, there is the opportunity for those people to consult with privacy experts. In some cases, the internal privacy office must sign-off, or the process must start with a meeting with the data protection staff. These experts can use their expertise and knowledge of prior privacy disasters to ask probing questions and identify areas where further consideration is required.

Evidence suggests that the quality of PIAs is enhanced where there is in-house privacy or data protection expertise involved in organisational decision-making at sufficiently high levels. There needs to be serious internal deliberations between program managers, IT security professionals and in-house privacy officers over privacy risks. It seems that the UK has a strong and extensive network of data protection officers throughout the public and private sectors, and can build on this significant experience.

3. Incentives and Business Processes

One of the major challenges in introducing PIAs will be ensuring that they are conducted in all circumstances that warrant one. Wonderful processes "on the books" are of little use unless PIAs are completed. While there are plenty of good reasons to conduct PIAs, individual and organisational inertia and attitudes toward regulation, competing demands and other forces will work against their completion. Incentives or other measures may be required in order to ensure that PIAs are completed when they should be.

In the absence of legislation or policy mandating the conduct of PIAs, incentives may be required to encourage their adoption or sanctions imposed when they are not conducted. At the very least, the proposed process must be perceived as of benefit to the organisation conducting the PIA, in relation to the effort and resources that go into it.

Where neither legislation nor policy absolutely mandates the conduct of PIAs (and in some cases, even when this exists), various jurisdictions have developed incentives or check-points where initiatives requiring PIAs can be identified and progress stopped. Technology procurement policy is one significant area where PIAs could be encouraged. While it is common to see the conduct or participation in a PIA as a deliverable for information technology systems involving personal information, procurement policy could play an "enforcement" role. It could require solicitations for certain types of initiatives to require a PIA as a deliverable.

We note, therefore, the potential for PIAs to be integrated into the existing Office of Government Commerce Gateway Review Process for Programmes and Projects. This appears to be the model being adopted by the Ontario Ministry of Government Services following a review of their PIA process, and it provides an excellent opportunity to inject privacy risk management into the assessment of programmes and projects at various stages of the life-cycle.

4. External expertise in consultancy and training

The quality of PIAs is largely based on the expertise of the people conducting them. Many jurisdictions rely on programme or business area staff who may not have sufficient grounding in privacy principles to recognise privacy issues, or sufficient familiarity with the legislation. They can be assisted, and the quality of PIAs improved, by guidance material, courses and consultation with experts. Because practitioners are not in the business of data protection, they will not likely be aware of "privacy disasters" and be able to recognise risk factors, and may not even be very familiar with applicable privacy regulations.

The conduct of PIAs in other jurisdictions is invariably dependent on the use of outside expertise for training and consultation. That outside expertise also needs to be nurtured. Although there is a large community of data protection expertise in the UK, there is always the danger that methodologies may be developed and marketed without sufficient care and expertise. Regardless of quality, quantity and helpfulness of guidance material, templates and tools provided, and of the data protection knowledge base, there is unlikely to be sufficient, existing expertise and assistance capacity within the UK to produce quality PIAs across the public and private sectors in the short to medium term.

Encouraging rapid implementation without consciously addressing the issue would risk setting a low baseline standard.

Training is therefore essential and usually accompanies or follows the introduction of a PIA process. In many jurisdictions, training in the conduct of PIAs is available on an ongoing basis. This can take the form of fairly traditional classroom training or be delivered electronically. The PIA process could be supported by the web-based PIA e-learning tool. This could provide a useful starting point for programme personnel to get to grips with PIA terminology and definitions. Education and training is a key component of successful integration of PIA processes into departmental and project workflows. Workshops, seminars and implementation seminars could support these initiatives.

The ICO need not necessarily develop or be the only provider of PIA training. The private sector may step in and develop training in the new UK PIA methodology when it is introduced. Those interested in this opportunity might include law firms and those companies already involved in delivering training of interest to public sector managers. Development of PIA training might happen on a sectoral basis, so instructors can be found who are experts in the field and have credibility. Industry umbrella organisations and trade associations might sponsor development of training in their field, or depending on their mandates, deliver it. Those involved in providing professional training and credentials (e.g. in the IT sector) may also feel that PIA modules would be beneficial additions to their offerings.

A United Kingdom PIA

With lessons learned from international experience in mind, and consideration of the UK context, the Handbook has been designed on the assumption that the following features should be incorporated into a United Kingdom PIA process. The process should:

1. Be a comprehensive risk analysis exercise
2. Be more process-oriented than output-oriented
3. Be integrated within existing management and business processes
4. Employ a screening tool
5. Provide flexibility of scale
6. Be transparent and accountable.
7. Define Organisational Responsibilities
8. Provide for External Review and Approval

1. Comprehensive

A comprehensive PIA involves privacy concepts beyond those entailed in data protection legislation. For instance, it might answer questions about the ethics of designing the initiative the way it is, looking at the incremental effects to surveillance it poses, etc. It should consider the reputation and economic risks of the initiative, as well as the legal risks. It should entail a search for and evaluation of less privacy-invasive alternatives and ways the negative impacts can be avoided or lessened. It should critically question the business need for privacy invasions, even when those are legal and likely to be accepted by the affected public.

2. Process Oriented

PIAs that are simply compliance checklists have a number of shortcomings and are bound to ignore larger, important questions. While no comprehensive PIA should be without a legal compliance checklist, it is not sufficient. For one thing, a checklist is a snapshot of the initiative as it is envisioned at the start of its implementation. It does not require consideration of function creep in the use of personal information or other things that might happen over time.

A PIA tool should not be overly focused on the form of the PIA end-product. Instead, it should focus on the types of analytical exercises to be conducted and the considerations which might lead organisations to conclude that the initiative under study could be improved from a privacy perspective.

3. Integrated into Existing Business and Management Processes

PIAs should not be regarded as separate from existing risk assessment strategies and tools. They should be part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes, as is common with other forms of threat/risk assessment. Incentives are created when project approval and/or funding is tied to the conduct of a PIA.

4. Screening Tool

An initial screening tool is one way to determine: a) whether a PIA needs to be completed: and b) the scale of the PIA to be conducted. A screening tool also allows appropriate resource allocation commensurate with the privacy risks.

5. Flexibility of Scale

A PIA process should afford the opportunity to vary the scale of the PIA – to choose between conducting full PIAs and smaller-scale PIAs, and tailor the analysis according to the circumstances. Guidance indicating the circumstances under which each type of PIA is appropriate should be provided, as should guidance about when and how thoroughly to conduct certain forms of information-gathering or analysis.

6. Transparent and Accountable.

The PIA process should include external consultation where appropriate, at a point where the direction of the initiative may be influenced, and reports should be published or otherwise made available. PIAs may be seen as irrelevant exercises in legitimation of initiatives in the absence of stakeholder consultation while there is still the opportunity for influencing the development of the initiative.

Even if external consultation cannot be conducted early in the development of the PIA because the initiative is being developed in secrecy, at some point, it will become public (e.g. after appropriate approvals) and the opportunity will arise to consult on the privacy aspects, even if it is at a later than optimal juncture.

7. Responsibility of the Organisation

Responsibility for the conduct of PIAs should lie with the organisation developing the initiative, with the assistance of internal and external experts as appropriate. In some cases, such as for large, high budget and high-privacy-risk initiatives, it may be appropriate to bring in outside privacy experts that operate somewhat independently and are able to draw the information they need about the initiative from the organisation. In other instances, programme staff may be able to complete large parts of the PIA, with

various, specialised types of analysis being conducted by in-house experts in privacy, policy and legal analysis, information systems security, etc.

The individual in the position responsible for compliance with data protection within the organisation should review the PIA. The senior executive who has responsibility for not only the initiative in question, but also the various parts of the organisation which will be involved in implementation should approve the PIA.

8. External review and approval

External review of a PIA by an organisation outside the PIA sponsor provides accountability, ensuring that PIAs are conducted and complete. This review also has the potential to provide value regarding privacy protection. However, review does not need to be mandated to be effective.

Regulators from both central agencies and privacy oversight offices report privacy improvements being made to initiatives as a result of their review of PIAs and the subsequent interaction with PIA sponsors.

Review should involve interaction between the regulator and the PIA sponsor, as questions or concerns are expressed by the reviewer and further information or alternatives are provided by the sponsor.

PRIVACY IMPACT ASSESSMENT BIBLIOGRAPHY

Secondary Literature

Anderson, Paige and Jim Dempsey. (2003) "Privacy and e-government: PIA and Privacy Commissioners – Two mechanisms for protecting privacy to promote citizen trust online" (Global Internet Policy Initiative) at: http://www.gipiproject.org/practices/030501pia.pdf

Bamberger, Kenneth A. and Deidre Mulligan (2007), "Privacy Decision-Making in Administrative Agencies," *Chicago Law Journal* forthcoming.

Bennett, Colin J. and Charles D. Raab. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press).

Bird, Jenny. (2003). *Privacy Impact Assessments: A Guide to the Best Approach for Your Organization, PRIVA-C*™ at: http://www.priva-c.com/includes/pdf/PRIVA-C%20Whitepaper%220Privacy%20Impact%20Assessments.pdf

Clarke, Roger. (2004) "A History of Privacy Impact Assessments" at: http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html

Clarke, Roger. (1999) "Privacy Impact Assessments," at: http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html

Flaherty, David H. *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989)

Flaherty, David H. (2001) "Privacy Impact Assessments: An Essential Tool for Data Protection," in S. Perrin, H. Black, D.H. Flaherty and T. M. Rankin *The Personal Information Protection and Electronic Documents Act* (Toronto: Irwin Law).

Hope-Tindall, Peter (2002) "PIA: Obligation or Opportunity –the choice is ours!" http://www.dataprivacy.com/mod/fileman/files/PIA_Material.pdf

Solove, Daniel. (2005) *The Digital Person* (New York: NYU Press)

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

_____ (1996b) 'PIAs - an early warning system' *Privacy Law & Policy Reporter* 3, 7 134-138, at: http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/65.html

_____. (1999) 'Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies' *Privacy Law & Policy Reporter* 5, 8 147-149 at: http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1999/8.html

_____ (2002) `Privacy impact assessment roundup' *Privacy Law & Policy Reporter* 9, 5 90-91: http://www.austlii.edu.au/au/journals/PLPR/2002/41.html

Waters, Nigel (2001) "Privacy Impact Assessment: Traps for the Unwary," *Privacy Law and Policy Reporter* 7, 9 at: http://www.austlii.edu.au/au/journals/PLPR/2001/10.html

White, Frank (2001) "The Use of Privacy Impact Assessments in Canada," *Privacy Files*, vol. 4, no. 7.

APPENDICES