PIAF

A Privacy Impact Assessment Framework for data protection and privacy rights

Deliverable D1

Editors:
David Wright, Trilateral Research & Consulting
Kush Wadhwa, Trilateral Research & Consulting
Paul De Hert, VUB-LSTS
Dariusz Kloza, VUB-LSTS

Prepared for the European Commission
Directorate General Justice

JLS/2009-2010/DAP/AG

21 September 2011

PIAF
PRIVACY IMPACT
ASSESSMENT FRAMEWORK

This report is the first deliverable from the PIAF consortium to the European Commission. All partners in the PIAF consortium contributed to this report. The contents of this report are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. The PIAF consortium consists of the following partners:

Partners	Partner short form	Country
Vrije Universiteit Brussel	VUB-LSTS	Belgium
Trilateral Research & Consulting	TRI	UK
Privacy International	PI	UK

Comments on this report are welcome and should be sent to:
david.wright@trilateralresearch.com

Contents

EXECUTIVE SUMMARY

This report reviews the privacy impact assessment (PIA) methodologies of seven countries and 10 PIA case studies. No other published report, to our knowledge, has done this. Thus, it represents the most complete compendium and analysis of PIA policies and practices yet compiled and published (on the PIAF website www.piafproject.eu). PIAF is the acronym for a Privacy Impact Assessment Framework.

The report is the first deliverable prepared for the European Commission's Directorate-General Justice under the Fundamental Rights and Citizenship Programme, Grant Agreement number: JUST/2010/FRAC/AG/1137 – 30-CE-0377117/00-70. The PIAF project kicked off in January 2011 and finishes in August 2012.

The timing of this report is rather felicitous because it comes a couple of months or so before the European Commission issues its proposed revisions to the data protection framework. The Commission has already signalled some of the changes we can expect in its Communication of 4 November 2010. One of the changes concerns "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data is being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms, or procedures, including profiling or video surveillance."[1]

Hence, European policy-makers and data protection authorities could benefit from this review and analysis of PIA in other countries, to construct a PIA methodology and policy that draws on the best elements of existing PIA practice.

The PIAF project is being undertaken by a consortium comprising Vrije Universiteit Brussel (VUB), Trilateral Research and Consulting, and Privacy International. In addition to our review and analysis of privacy impact assessment methodologies in Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and US, the consortium has drawn conclusions and made some initial recommendations for an optimised privacy impact assessment framework for Europe.

There are various definitions of PIA, but we define a privacy impact assessment as a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a *process* which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project.[2] It is a process that should continue until and even after the project has been deployed.

Just as there different definitions of privacy impact assessment, there are differences (as well as similarities) in the PIA methodologies employed in the seven countries covered in this

[1] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[2] The word "project" is used in this paper in its widest sense, to include any technology, product, service, programme, policy or initiative that may impact upon privacy.

report. Each of the existing methodologies has some good points, but also shortcomings. This report reviews the following methodologies:

Australia

The Office of the Privacy Commissioner (OPC) published its *Privacy Impact Assessment Guide* in August 2006, and a revised version in May 2010.[3] The *Guide* is addressed to those who undertake a PIA, no matter whether they are from government agencies, the private sector or not-for-profit sector (i.e., civil society organisations). This is an important point to note. Any organisation, from whatever sector, should undertake a PIA if it is planning a project that might pose risks to privacy. However, there is no legislative requirement in Australia to conduct a PIA. It does not impose a particular PIA style ("There is no one-size-fits-all PIA model.") but suggests a flexible approach depending on the nature of the project and the information collected.

Another important distinction between the Australian PIA Guide and some of its counterparts is that it makes the point (at p. iii) that information privacy is only one aspect of privacy. Other types of privacy include bodily privacy, territorial privacy and communications privacy.[4]

It defines a project as "any proposal, review, system, database, program, application, service or initiative that includes handling of personal information". The ICO *PIA Handbook* uses a similar definition. Note that the definition excludes proposed policies or legislation. The *PIA Guide* says (p. viii) a PIA should be an integral part of the project from the beginning. A PIA should evolve with and help shape the project, which will help ensure that privacy is "built in" rather than "bolted on" (which echoes the same wording used in the ICO *PIA Handbook*).

The *PIA Guide* says (p. x) that "Consultation with key stakeholders is basic to the PIA process." The Privacy Commission encourages organisations, "where appropriate", to make the PIA findings available to the public (p. xviii).[5] The PIA Guide says (p. x) publication "adds value; demonstrates to stakeholders and the community that the project has undergone critical privacy analysis; contributes to the transparency of the project's development and intent".

Victoria

Roger Clarke has described the PIA guide produced by the Office of the Victorian Privacy Commissioner (OVPC) as "one of the three most useful guidance documents available in any

[3] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, Sydney, NSW, August 2006, revised May 2010. http://www.privacy.gov.au. The *PIA Guide* can also be downloaded from http://www.oaic.gov.au/publications/guidelines.html#privacy_guidelines.

[4] Roger Clarke distinguished these different types some years ago. See Clarke, Roger, "What's privacy?", 2006. http://www.rogerclarke.com/DV/Privacy.html

[5] The Privacy Commissioner acknowledges (p. xviii) that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part. However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the Commissioner encourages organisations to consider the release of a summary version.

jurisdiction, anywhere in the world".[6] The current OVPC *PIA Guide* dates from April 2009. It is the second edition of the guide originally published in August 2004.

The OVPC *PIA Guide* is primarily aimed at the Victorian public sector, but it says it may assist anyone undertaking a PIA. Like the Australian OPC *Guide*, it says that privacy considerations must be broader than just information privacy; bodily, territorial, locational and communications privacy must also be considered.

It sets out various risks thematically linked to Victoria's privacy principles as well as possible strategies for mitigating those risks. A template provides the structure of a PIA report, which the user can adapt to his or her circumstances.

The Guide uses (p. 5) the word "project" to encompass any type of proposed undertaking, including "legislation" and "policy", which are not mentioned in the Australian OPC *Guide*.

The Guide says (p. 6) up-front commitment from an organisation's executive to the conduct of PIAs is needed to ensure buy-in to the PIA's eventual recommendations. The Guide advocates publication of the PIA report.

Like most other guidance documents, the *Guide* says that a PIA should assess not only a project's strict compliance with privacy and related laws, but also public concerns about the wider implications of the project. It cites the New Zealand *PIA Handb*ook which notes that "Proposals may be subject to public criticism even where the requirements of the Act have been met. If people perceive their privacy is seriously at risk, they are unlikely to be satisfied by (an organisation) which justifies its actions merely by pointing out that technically it has not breached the law."[7]

The *Guide* says that public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence amongst the public that their privacy has been considered. Public consultation may generate new options or ideas for dealing with a policy problem. If wide public consultation is not an option, the *Guide* says the organisation could consult key stakeholders who represent the project's client base or the wider public interest or who have expertise in privacy, human rights and civil liberties.

Canada

In Canada, policy responsibility for privacy impact assessment in the federal government lies with the Treasury Board of Canada Secretariat (TBS), which defines PIA as "a policy process for identifying, assessing and mitigating privacy risks".[8] TBS promulgated a new Directive on Privacy Impact Assessment in April 2010.[9]

The directive ties PIAs with submissions to the Treasury Board for program approval and funding. This is one of the strongest features of Canadian PIA policy. PIAs have to be signed off by senior officials, which is good for ensuring accountability, before a submission is made

[6] Clarke, Roger, "PIAs in Australia: A work-in-progress report", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
[7] Office of the Privacy Commissioner (New Zealand), *Privacy Impact Assessment Handbook*, June 2007, p.24
[8] Treasury Board of Canada Secretariat, Policy on Privacy Protection, Ottawa, 1 Apr 2008. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text
[9] Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 Apr 2010. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text

to the Treasury Board. The PIA is to be "simultaneously" provided to the Office of the Privacy Commissioner. Institutions are instructed to make parts of the PIA publicly available. Exceptions to public release are permitted for security as well as "any other confidentiality or legal consideration". Heads of government institutions are responsible for monitoring and reporting their compliance with the PIA directive and the TBS "will monitor compliance with all aspects of this policy".

The TBS does not approve PIAs; it only reviews them to ensure that "the assessment is complete". The TBS requirements convey to the reader that the emphasis is on completion of a PIA report, rather than PIA as a process. The directive makes no provision for stakeholder engagement. Nor does it address the benefits of undertaking a PIA and finding solutions to privacy risks[10].

While the directive does not refer to the TBS's PIA Guidelines[11], these are still recommended even if they have not been revised since August 2002.

The TBS PIA Guidelines are based upon privacy principles, i.e., those in the Canadian Standards Association's *Model Code for the Protection of Personal Information*[12] as well as federal privacy legislation and policies.

The Guidelines include two questionnaires to help identify privacy risks or vulnerabilities in the proposal and to facilitate the privacy analysis. The Guidelines say that departments and agencies can undertake generic or overarching PIAs where proposals are similar or interrelated to avoid duplication of effort.

Ontario

In Ontario, since the late 1990s, the principal driver behind government policy in relation to PIAs was not the privacy oversight body, but a central agency called the Management Board Secretariat (MBS). As early as June 1998, a completed PIA became a pre-requisite for approval of Information and Information Technology (I&IT) project plans submitted for Cabinet approval.[13]

In December 2010, Ontario's central agency, the Office of the Information and Privacy Commissioner released a revised PIA guide, replacing the 2001 version. The guide provides an overview of the PIA methodology and outlines the privacy activities required throughout a project's lifecycle. It also explains how to integrate a PIA into project management and use the results to meet the corporate governance requirements. Three PIA tools were also released at that time and provide detailed instructions, checklists, templates and other resources to help projects complete the PIA process. It is too early to draw conclusions on their use. [14]

[10] Although the PIA Directive does not mention benefits or solutions, the PIA Guidelines do mention potential outcomes, which can be regarded as benefits or solutions.

[11] Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks*, Ottawa, 31 August 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp.

[12] http://www.csa.ca/cm/ca/en/privacy-code

[13] Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", *Computer Law & Security Review*, Vol. 25, No.2, April 2009, pp. 123-135 [p. 127]. PrePrint at http://www.rogerclarke.com/DV/PIAHist-08.html

[14] Bayley, Robin, and Colin J. Bennett, "Privacy impact assessments in Canada", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

Section 6 of the Regulation to the Personal Health Information Protection Act (PHIPA) mandates PIAs for Health Information Network Providers (HINP), when two or more Heath Information Custodians (HIC) use electronic means to disclose Personal Health Information (PHI) to one another.[15]

The *Privacy Impact Assessment Guide* for the Ontario Public Service (hereafter PIA Guide)[16] says ultimate accountability for privacy protection rests with the Minister, as head of each government institution.[17]

The Guide defines privacy impact assessment as "a consistent and systematic approach for identifying and analysing privacy risks when changing or developing programs or systems".[18] It is also described as "both a due diligence exercise and a risk management tool".

The Guide says it is important to look at other types of privacy when assessing a project, i.e., freedom in the physical domain, freedom of movement or expression or of the person or personal space; freedom to communicate privately with others; freedom to determine when, what, how and with whom they share their personal information. It adds that "An activity may comply with the law but still be seen as unnecessarily privacy invasive."[19]

It states that "The potential damage to the individual must take precedence in your assessment over organizational risks."[20] It also adds that "Risk management can mitigate a risk, but it can never be completely avoided or eliminated. If your project involves personal information, there always will be some privacy risk."

Alberta

In 2001, the Office of the Information and Privacy Commissioner (OIPC) of Alberta introduced its first Privacy Impact Assessment (PIA) questionnaire. In the following eight years, according to the OIPC, the practice of privacy impact assessments matured and the number of PIAs increased dramatically. In January 2009, the OIPC revised the PIA template and guidelines.[21]

Those submitting PIAs are told to consider the feedback from the OIPC before they implement their projects. Otherwise, if the OIPC identifies privacy concerns, "it may be necessary to make expensive and time-consuming changes to your project late in the development cycle".[22] The OIPC appears to exercise much more power than most of its counterparts. Not only are PIAs mandatory, they must be submitted to the OIPC before implementation of a new system or practice. If the OIPC finds shortcomings, projects can be

[15] Tancock, David, Siani Pearson and Andrew Charlesworth, "Analysis of Privacy Impact Assessments within Major Jurisdictions", in *Proceedings of the 2010 Eighth Annual International Conference on Privacy, Security and Trust*, Ottawa, 17-19 Aug 2010, published 30 Sept 2010, pp. 118-125 [p. 121]. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5593260

[16] Office of the Chief Information and Privacy Officer (OCIPO), *Privacy Impact Assessment Guide for the Ontario Public Service*, Queen's Printer for Ontario, December 2010.

[17] Ontario PIA Guide, p. 4.

[18] Ibid., p. 5.

[19] Ibid., p. 37.

[20] Ibid., p. 48.

[21] Office of the Information and Privacy Commissioner (OIPC) of Alberta, *Privacy Impact Assessment (PIA) Requirements*, For use with the Health Information Act, January 2009. www.OIPC.ab.ca

[22] OIPC, 2009, p. 5.

turned down or forced to make costly retrofits. It appears to play a much more activist role in reviewing PIAs.

The OIPC points out that "acceptance" of a PIA is not approval. It only reflects the OIPC's opinion that the project manager has considered the requirements of the HIA and has made a reasonable effort to protect privacy.

The OIPC says custodians should review their PIAs as new practices and technologies evolve after projects are implemented and new threats to privacy may also develop. Custodians should advise the OIPC of any resulting changes to the PIA. The OIPC says if a member of the public makes a complaint against the custodian's organisation, it may review previously submitted PIAs.[23]

Unlike other PIA methodologies that say PIAs should be initiated as early as possible, the OIPC PIA Requirements say that, generally speaking, the best stage to do a PIA is after all business requirements and major features of the project have been determined in principle, but before completing detailed design or development work to implement those requirements and features, when it is still possible to influence project design from a privacy perspective.[24]

The Alberta PIA Requirements are unusual in making mandatory the format for HIA PIAs.

Ireland

The Health Information and Quality Authority is an independent authority, established under the Health Act 2007, to drive improvement in Ireland's health and social care services. Among other things, it aims to ensure that service users' interests are protected, including their right to privacy, confidentiality and security of their personal health information. In this context, the Authority produced a PIA Guidance in December 2010[25] following its review of PIA practice in other jurisdictions,[26] which found a growing convergence in what constitutes best practice in relation to PIAs.

The Guidance says the primary purpose in undertaking a privacy impact assessment is to protect the rights of service users. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks.

It says that a PIA in its own right may not highlight all privacy risks or issues associated with an initiative. A PIA depends on service providers having the correct processes in place to carry out the PIA. These include identification of the correct stakeholders for the assessment, and involvement of senior managers in order to implement the PIA recommendations. It is essential that the PIA is regularly updated to reflect any changes to the direction of the initiative.

The PIA should generally be undertaken by the project team. The service provider is ultimately responsible for the completion of the PIA and for implementing any changes to the

[23] OIPC, 2009, p. 6.
[24] OIPC, 2009, p. 13.
[25] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010. http://www.hiqa.ie/resource-centre/professionals
[26] Health Information and Quality Authority, *International Review of Privacy Impact Assessments,* 2010. http://www.hiqa.ie/standards/information-governance/health-information-governance

project plan following recommendations from the PIA. PIAs should be reviewed and approved at a senior level with each PIA report being quality assured by senior management.

Like the Alberta PIA Requirements, the Irish Guidance says that if a PIA is conducted too early, the results will be vague as there may not be enough information available about the project, its scope and proposed information flows to properly consider the privacy implications and as such the PIA may need to be revisited. The PIA process should be undertaken when a project proposal is in place but before any significant progress or investment has been made. The findings and recommendations of the PIA should influence the final detail and design of the project.[27]

The project manager should explain the option(s) chosen for each risk and the reasoning behind the choices. If there is a residual or remaining risk, which cannot be mitigated, the project team must decide whether or not it is acceptable to continue with the project.

The Health Information and Quality Authority favours publication of PIA reports as it builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information. Completed PIA reports should be presented in a reader-friendly format.[28]

New Zealand

The origins of privacy impact assessment in New Zealand date back to at least 1993, to the legislative requirement under section 98 of the Privacy Act 1993[29] to undertake Information Matching Privacy Impact Assessments (IMPIAs).[30] IMPIAs are legally mandatory assessments involving an examination of legislative proposals that provide for the collection or disclosure of personal information and used for an information-matching programme[31] in terms of the information-matching guidelines.[32] The Office of the Privacy Commissioner (OPC) issued guidance on their implementation in 1999.[33]

The OPC published a PIA Handbook in October 2002[34] (reprinted in 2007).[35] The Handbook defines a PIA as a "systematic process for evaluating a proposal in terms of its impact upon privacy", which can help an agency to identify the potential effects of a proposal on individual privacy, examine how any detrimental privacy effects can be overcome and ensure that new projects comply with the information privacy principles. A PIA is thus, a "valuable tool for businesses and governments which take privacy seriously".[36]

---

[27] Ibid., p. 18.
[28] Authority, pp. 17-32.
[29] Superseding the Privacy Commissioner Act 1991.
[30] For contents of IMPIAs, see Office of the Privacy Commissioner, Guidance Note for Departments Seeking Legislative Provision for Information Matching, 16 May 2008, Appendix B. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching/#appendix
[31] See Office of the Privacy Commissioner, Operating programmes, 30 June 2010. http://privacy.org.nz/operating-programmes/
[32] Set out in section 98 of the Privacy Act 1993.
[33] Office of the Privacy Commissioner, Guidance Note for Departments Seeking Legislative Provision for Information Matching, 16 May 2008. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching (current version)
[34] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Wellington, 2002.
[35] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Auckland/Wellington, 2007 [hereafter, the NZ PIA Handbook]. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf
[36] Ibid., p. 3.

The Handbook offers (pp. 21-28) in-depth practical advice on how to prepare privacy impact reports.

The Handbook recommends (p. 14) minimising the duplication of PIA efforts by undertaking generic or overarching PIAs where planned projects are very similar. It recommends (p. 21) that the PIA report is best written with a non-technical audience in mind and that it be made publicly available (p. 19) (either in full or summary on an organisation's website).

The Handbook mentions consultation with stakeholders (p. 26) but does not outline the consultative process. The agency conducting the PIA may consult the Privacy Commissioner. It may receive the PIA report for information only or offer feedback and constructive suggestions. PIAs are generally not mandatory in New Zealand, however, section 32 of the Immigration Act 2009[37] explicitly requires PIA be conducted if biometric information are processed.

United Kingdom

The Information Commissioner's Office (ICO) is credited with launching privacy impact assessment in the UK. In 2007, the ICO commissioned a team of experts co-ordinated by Loughborough University to study PIAs in other jurisdictions (Australia, Canada, Hong Kong, New Zealand and the United States) and identify lessons to guide PIAs in the UK.[38] In 2007, the ICO published a PIA handbook[39] and became the first country in Europe to do so. The ICO published a revised version in June 2009.[40]

According to the ICO, a PIA is "a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions."

The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start".[41] It accepted the value of PIA reports and stressed that they will be used and monitored in all departments. PIAs have thus become a "mandatory minimum measure".[42]

[37] Immigration Act 2009, Public Act 2009 No 51.
http://www.legislation.govt.nz/act/public/2009/0051/latest/096be8ed806837b3.pdf

[38] ICO, *Privacy Impact Assessments: International Study of their Application and Effects*, Information Commissioner's Office, Wilmslow, Cheshire, UK, December 2007.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf

[39] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 1.0, December 2007.

[40] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009 [hereafter ICO Handbook 2009].
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html,
http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

[41] Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008, p. 18.
http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

[42] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews". http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

The Handbook places responsibility for managing a PIA at the senior executive level (preferably someone with lead responsibility for risk management, audit or compliance).

The ICO does not play a formal role in conducting, approving or signing off PIA reports. It does, however, play an informative and consultative role in supporting organisations in the conduct of PIAs.

The ICO views the PIA process as including identification of and consultation with stakeholders. It distinguishes between a full-scale PIA for large and complex projects and a small-scale PIA for smaller projects.

Roger Clarke has described the UK ICO Handbook as one of the "best practice publications".[43] Despite this, Warren and Charlesworth contend that there are several problems with the UK PIA system, one of which is the lack of review and oversight.[44] They also point out the "apparent lack of PIA cross-fertilization across departmental boundaries" and the "relatively 'hands-off' oversight" raises doubts about the efficacy of governmental PIA processes.[45] They also point out that there is no formal process of external review of PIAs in the UK by central agencies or by the ICO (which functions largely as an advisory body in this respect).

Warren and Charlesworth note that, in the UK, as in other places, there is:

- no consistent process for ensuring effective consultation with stakeholders, notably the general public, e.g., a register of ongoing PIAs, consultation periods and relevant contact details;
- no consistency in reporting formats for PIAs, whether in draft or completed, e.g., a PIA might be reported in a detailed 62-page document, or simply mentioned in a paragraph in a general impact statement[46]; and,
- no strategy for ensuing that, where PIA decisions and reports are made publicly available, they are easily accessible, perhaps from a centralised point, e.g., the UK Office of Public Sector Information (OPSI) or the ICO.[47]

United States

In the United States, privacy impact assessments for government agencies are mandated under the E-Government Act of 2002. This Act states that PIAs must be conducted for new or substantially changed programmes which use personally identifiable information. Personally identifiable information (PII) is defined as "any information that permits the identity of an individual to be directly or indirectly inferred."[48] The processing of PII in the US is also covered by Fair Information Practice Principles (FIPP) from the Privacy Act of 1974.

[43] Clarke op. cit., 2011. Note, Clarke was lead author on the team that drafted the Information Commissioner's 2007 PIA Handbook.
[44] Warren, Adam, and Andrew Charlesworth, "Privacy Impact Assessment in the UK" in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
[45] Ibid., op. cit., 2012.
[46] See, for example: Department of Communities and Local Government, *Making Better Use of Energy Performance Data: Impact Assessment*, Consultation, March 2010.
http://www.communities.gov.uk/documents/planningandbuilding/pdf/1491281.pdf. Department for Transport, *Impact Assessment on the Use of Security Scanners at UK Airports*, Consultation, March 2010.
http://www.dft.gov.uk/consultations/closed/2010-23/ia.pdf
[47] Warren and Charlesworth, op. cit., 2012
[48] Department of Homeland Security, *Privacy Technology Implementation Guide*, 16 Aug 2007, p. 8.

Section 208 of the E-Government Act requires that PIAs must be reviewed by a chief information officer or equivalent official, and should be made public, unless it is necessary to protect classified, sensitive or private information contained in the assessment. Agencies are expected to provide their Director with a copy of the PIA for each system for which funding is requested. Each agency Director must issue guidance to their agency specifying the contents required of a PIA.[49]

Additionally, the creation of the Department of Homeland Security (DHS) via the Homeland Security Act of 2002 mandates that the DHS conduct privacy impact assessments and creates a Chief Information Officer position with responsibility for these privacy assessments.

On 26 Sept 2003, the Office of Management and Budget (OMB) issued a Memorandum to heads of Executive departments and agencies providing guidance for implementing the privacy provisions of the E-Government Act, as required by section 208 of the Act.[50] The OMB specifies what must be in a PIA and, in doing so, it puts an implicit emphasis on the end product, the report, rather than on the process of conducting a PIA.

The PIA document is to be made publicly available. However, agencies are not obliged to make the PIA or a summary publicly available if publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest). Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

Homeland Security

The Department of Homeland Security PIA guidance has undergone a number of revisions, and the most recent version, which is discussed here, is the 2010 version.

The Department of Homeland Security Act states that the DHS Privacy Officer should also conduct a PIA in situations where one is not required by the E-Government Act, for example, in respect of proposed department rulemaking, to ensure that new rules do not adversely affect privacy, for national security systems, to ensure that such secret programmes appropriately consider and implement privacy protections and for human resources information systems.[51]

The guidance describes the PIA as a "living document", which needs to be updated regularly as systems and processes are changed and updated. Here, the DHS appears to focus on PIA as a process, rather than an end result.

The use of a PIA as a form of public engagement is cited in a number of paragraphs in the PIA guidance document. The PIA guidance notes and the associated PIA Template[52] describe the components of a DHS PIA. In one of these, officials must describe the procedures to allow

[49] E-government Act of 2002 , Pub.L.107-347.
[50] Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Washington, DC, 26 Sept 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html
[51] Teufel III, Hugo, *Privacy Policy and Guidance Memorandum*, Department of Homeland Security, Memorandum Number 2008-02, 30 Dec 2008.
[52] DHS, *Privacy Impact Assessment Template*, 2010.

individuals access to their information and correct inaccurate information. Officials must also describe how the project notifies individuals about the procedures for correcting information. Another section discusses auditing and accountability.

Unlike other agencies, the DHS has an external oversight body that evaluates PIAs and other privacy activities.

Auditing PIAs

Even scarcer than actual PIA reports are audits of PIA reports and practice. The principal (and perhaps only publicly available) audits are those undertaken by the Office of the Privacy Commissioner of Canada (OPC) and the Government Accountability Office (GAO) in the US.

Following its major audit of government institutions' PIAs in 2007, the Office of the Privacy Commissioner in Canada said in its report that "the PIA process was far from being fully integrated into the overall risk management strategies of individual entities". The most common control weakness identified within the management systems reviewed was the lack of a mandatory and formal screening process for all programs, services, plans and policies to identify potential PIA candidates.[53]

In its recommendations, the OPC said that beyond having the necessary resource capacity to implement the PIA policy, the single most important determinant of success is the existence of a sound management control framework. It recommended that deputy heads of all government institutions should ensure that their organisation has an adequate administrative infrastructure to

- Identify and document all proposals that may present privacy risks;
- Establish a sound structure for organizational accountability;
- Develop and implement a system to track all proposals subject to the PIA policy, and the detailed PIAs conducted;
- Provide guidance and training to managers and staff; and
- Establish quality control, consultation, communication, follow-up and evaluation procedures for PIA.[54]

It recommended that the internal audit branches of all federal institutions should include privacy and PIA related reviews in their plans and priorities in the future. [55] It saw a need for a federal privacy assessment registry, to provide a single window of access to PIAs across government. The registry could be used by the public to better understand the substance and privacy impacts of government projects and by institutions such as the Treasury Board Secretariat and the Privacy Commissioner to monitor PIA activities. [56]

The OPC commented that "enhancing the transparency of the privacy impact assessment process is critical to improving the quality of privacy analysis in government. Greater scrutiny generated by public exposure can prompt greater care in the preparation of PIAs and provide

[53] Ibid., p. 14.
[54] Privacy Commissioner of Canada, *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report, October 2007, p. 22. http://www.priv.gc.ca/information/pub/ar-vr/pia_200710_e.cfm
[55] OPC, 2007, p. 27.
[56] OPC, 2007, pp. 28-29.

Parliament and the public with the necessary information to have more informed debates concerning privacy protection."[57]

Independent, third-party assessment of PIAs in the US government agencies are made by OMB reports to Congress and the GAO. For example, in a review of data mining applications by five different federal agencies, the GAO found that only three of the five agencies examined had carried out a PIA (although one was exempt), and that "none of these assessments adequately addressed all the statutory requirements".[58] A further GAO report noted a number of failures to comply with privacy requirements for programmes that were covered by the E-Government Act.[59]

The issues uncovered in audits by the GAO demonstrate a number of shortcomings inherent in the US PIA system as it is currently designed and implemented. PIA experts have identified three different specific shortcomings of the US PIA: its lack of public consultation mechanisms, the compliance only orientation of the process and, relatedly, the fact that the PIA is a living document in name only. However, despite these shortcomings, privacy experts have also noted that the US PIA does effectively assist in considering privacy in the public sector and enables agencies to work towards improvements in their system design.

Roger Clarke concludes that government agencies have subverted PIAs to a legal compliance study and private corporations do not adequately address privacy issues, which has serious implications due to their privileged position in the global economy.[60]

* * *

In addition to this executive summary of PIA methodologies in the seven countries, we encourage readers who do not have time to read the full report to read the Conclusions (Chapter 10).

[57] OPC, 2007, p. 29.
[58] Government Accountability Office, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866, Aug 2005, p. 25. http://www.gao.gov/new.items/d05866.pdf
[59] GAO, op. cit., 2005, p. 27.
[60] Clarke, op. cit., 2009, p. 130.

1 INTRODUCTION

PIAF is the acronym for a Privacy Impact Assessment Framework for data protection and privacy rights. The PIAF project is being completed with co-funding under the EU's Fundamental Rights and Citizenship Programme. The PIAF project is being undertaken by a consortium comprising Vrije Universiteit Brussel (VUB), Trilateral Research & Consulting and Privacy International. VUB is the co-ordinator. The project began in January 2011 and concludes in August 2012.

1.1 OBJECTIVES

The overall goal of this project is to encourage the European Commission and Member States to adopt a progressive privacy impact assessment policy as a means of addressing many of the needs of and challenges to the Information Society and, particularly, as a means of engaging with and empowering stakeholders, including the public, in the decision-making process with regard to any technology, project, service, policy or programme which could impact privacy.

Among these needs and challenges are those involving the free circulation of information based on the protection of the individual's right to privacy, reinforcing children's privacy, risks posed by the Internet, surveillance, awareness of data protection and privacy risks, and use of privacy enhancing technologies.

The main objectives of the project are as follows:

1. To provide an overview of privacy impact assessment practices in those countries that already carry out PIAs, i.e., Australia, Canada, Hong Kong, New Zealand, the US and UK, and to identify the best elements of each which could be used in constructing a model framework, a PIA policy for the European Union (both at EU level and in the MS) and to perform an analysis of 10 actual privacy impact assessments.

2. To conduct empirical research with regard to the factors affecting the adoption of a PIA policy in each of the EU Member States and, in particular, to understand the acceptability of the best elements as identified in the first objective. The empirical research will be based on a combination of telephone interviews and a written questionnaire.

3. To provide an analysis of the empirical research and to make recommendations to the European Commission, Member States and industry with regard to a progressive privacy impact assessment policy. Among other things, the recommendations will also include reference to specific needs of and challenges to the Information Society, including the application of the PIAs to transborder flows of personal data.

4. To conduct an awareness raising campaign, particularly targeting data protection authorities, policy-makers and industry, with regard to the findings of each phase of this proposed project, to encourage the Commission and Member States to adopt a progressive privacy impact assessment policy and to disseminate the results of the project.

This project aims to reach out to these **stakeholders**:

- Policy-makers at the European and Member State levels and, in particular, those responsible for initiating the adoption of a privacy impact assessment policy;

- Data protection authorities;
- Other government departments who would be called upon to use PIAs, preferably whenever submissions are made for any new policy, programme, database or other scheme involving the use of personal data;
- Industry, particularly those prominent in the Information Society, with the aim of convincing them that it is in their interest as a matter of good risk management practice, to use PIAs whenever they initiate or make significant changes to technologies, products or services involving the use of personal data;
- Civil society organisations, especially those that take an interest in privacy and data protection issues;
- The media, who are helpful in raising public awareness of privacy and data protection issues;
- Academia, especially those experts in privacy and data protection issues, who can act as leverage in promulgating the results of this project;
- The public, who until now have had few or no opportunities to participate directly in the decision-making process with regard to the development of new technologies, services, products, policies, databases or other schemes that make use of their personal data.

1.2 DEFINITION OF PRIVACY IMPACT ASSESSMENT

Although there are many definitions of privacy impact assessment, we define the term as follows:

A **privacy impact assessment** is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts.[1]

A PIA is more than a tool: it is a *process* which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed. A good PIA will engage stakeholders from the outset as a way of gathering their views and ideas about how any intrusive privacy impacts can be avoided or mitigated.

1.3 GROWING INTEREST IN PIAS

In a way, PIAs are the culmination, in the privacy protection field, of social, political and legal processes of more than 50 years. Their distant ancestors are environmental impact assessments, that (in their US form of "Environmental Impact Statements") originated in the "green" movements of the 1960s. The positive experience of environmental impact assessments led to social impact assessments (SIAs) that themselves became established by the 1980s. SIAs aim at ensuring that developments or planned interventions maximise the benefits and minimise the costs of those developments, including, especially, costs borne by the community.

[1] This is the definition adopted in Wright, David, and Paul De Hert, "Introduction to privacy impact assessment" in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming]. The chapter refers to other definitions of PIA as well. Although the wording of these definitions varies, there is a high degree of commonality with regard to what a PIA is and what it is supposed to do.

The concept of a PIA emerged and grew in Australia, Canada, Hong Kong, New Zealand and the United States from about the mid-1990s. In December 2007, the UK became the first country in Europe to publish a privacy impact assessment manual. Although there are differences in the way in which privacy impact assessments are conducted in these countries, a PIA may be defined as a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects.

Article 20 of the European Data Protection Directive may be regarded as having some kinship with a PIA. Article 20 says in part that "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." However, the European Commission seems to want something more than this. In Article 4 of its RFID Recommendation, the Commission called upon Member States to "ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments".

The so-called Madrid Resolution adopted by the last International Conference of Privacy and Data Protection Commissioners in November 2009 encourages "The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing".

Jacob Kohnstamm, Chairman of the Dutch Data Protection Authority and now Chair of the Article 29 Working Party, has said "Data controllers can and should make use of … privacy impact assessments".[2]

In its 4 November 2010 Communication, the European Commission said it will examine the the possibility of including in its legal framework (a revised EU Data Protection Directive) "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance".[3]

In February 2011, the Article 29 Working Party approved the RFID PIA Framework developed by industry following the above mentioned Recommendation from the Commission.

These are just a few of the indications of the growing interest in PIAs in Europe.

[2] "Data controllers should be able to demonstrate their capacity and responsibility to achieve privacy objectives and to determine appropriate and effective measures to reach those goals. Data controllers can and should make use of all kinds of instruments, such as privacy impact assessments, audits and privacy enhancing technologies in order to accomplish this." Kohnstamm, Jacob, "Introductory words", Speech by the Chairman of the Dutch DPA at the Safe Harbour Conference, Washington, 17-18 Nov 2009.
http://www.dutchdpa.nl/Pages/en_med_20091118_SafeHarbour.aspx

[3] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010.
http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

Although the concept of PIAs is not unknown in Europe, Europe as a whole has not progressed so far as Australia, Canada, Ireland, New Zealand, the United Kingdom and the United States in the development and implementation of PIA policy and practice. Be that as it may, Europe does, however, have the opportunity to consider an in-depth examination of PIA practices in those countries, to draw upon the best elements of their practices and to craft an even more effective PIA policy to address the vexing problems and challenges to privacy and data protection in the Information Society.

While it is relatively straightforward to conduct an in-depth study of existing PIA use in the aforementioned countries, what is rather more problematic is determining whether there are any conditions or factors or political or economic sentiments in the Member States that would affect the adoption of a privacy impact assessment policy -- and not just any policy, but a progressive one that is comprehensive in scope, that offers transparency and earns credibility among all stakeholders.

Among the key, potentially problematic questions are these: Should privacy impact assessments be mandatory (as they are in Canada, the UK and US) for government departments? Should they be mandatory for industry? How would or should application of privacy impact assessments be conducted on transborder "projects" (in the widest sense of the word)? How should privacy impact assessments be optimised? Should companies be obliged to engage stakeholders in the PIA process? Should privacy impact assessments be published on organisations' websites?

1.4 PRIVATE SECTOR PIAS

Privacy impact assessments have been most frequently used by government departments and agencies, but they are beginning to be used in the private sector as well, sometimes because they are required by government policy, but at other times because companies recognise that PIAs are a form of risk management and are folded into the risk management process. This is true of companies such as Nokia, Siemens and Vodafone.[4]

Evidence of the growing private sector use of PIA includes the following:

In Australia, although PIAs are not required by law, the Office of the Privacy Commissioner (OPC) produced a *Privacy Impact Assessment Guide*, revised in May 2010, explicitly aimed at companies as well as governmental bodies.[5]

In Canada, the Alberta government requires that companies perform PIAs if they are regarded as "custodians" of personal health information, under section 64 of the Health Information Act, which came into force in 1999. The requirement covers any "proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information [that] may affect the privacy of the individual who is the subject of the information".

[4] See chapters 11 – 13 in Wright and DeHert, op. cit., 2012 [forthcoming].
[5] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, Sydney, NSW, August 2006, revised May 2010. http://www.privacy.gov.au. The *PIA Guide* can also be downloaded from http://www.oaic.gov.au/publications/guidelines.html#privacy_guidelines.

The PIA Handbook, first published by New Zealand's Privacy Commissioner in October 2002[6], describes PIA as a "valuable tool for businesses and governments".[7] Google undertook a PIA (see section 9.7) at the behest of the NZ Privacy Commissioner with regard to its Street View service.

The International Organization for Standardization has developed a voluntary consensus PIA standard (ISO 22307:2008) applicable to financial services companies.

The RFID industry has developed an RFID PIA Framework[8], which was approved by the Article 29 Data Protection Working Party in February 2011[9] and had been prompted by the European Commission's RFID Recommendation.[10]

The Commission's proposed revision of the data protection framework in Europe would be applicable to the private sector as well the public and voluntary sectors and, if it proceeds as indicated in its Communication of 4 November 2010, will make PIA mandatory in some instances. This will significantly expand the requirement for PIAs by the private sector.

Bayley and Bennett have commented that private sector PIAs are most frequently conducted for information technology projects. PIAs have been conducted by telecommunications companies, those providing back-room services in human resources and payment processing, banks and other financial institutions, international energy companies and major retailers. PIAs are also spreading from public to private sectors through contracting out, public-private partnerships and other joint initiatives, particularly in the health care field with shared information systems. PIAs may also be conducted by those seeking access to publicly held information as a due diligence exercise before information sharing agreements are concluded. Some organisations recognise that privacy can give them a strategic advantage. Others conduct PIAs as a risk management process, recognising that business can be affected by privacy incidents such as breaches and complaints.[11]

We have chosen 10 PIA reports, two each from the leading PIA countries – Australia, Canada, New Zealand, the UK and US. One can find quite a few (relatively speaking) PIA reports from Australia and the US, PIA summaries from Canada, but rather fewer PIA reports from the UK.

We assume most companies and even governments are afraid to make their PIA reports public, probably because they are afraid of criticism – i.e., they don't want the citizens or consumers to be aware of the risks to privacy posed by their project or other initiative.

---

[6] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Auckland/Wellington, 2007 [hereafter, the NZ PIA Handbook].
http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf

[7] Ibid., p. 3.

[8] Privacy and Data Protection Impact Assessment Framework for RFID Applications [the "PIA Framework" hereafter], 11 February 2011, p. 3. http://cordis.europa.eu/fp7/ict/enet/policy_en.html

[9] Art. 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Brussels, 11 February 2011.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

[10] European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009.
http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

[11] Bayley, Robin, and Colin J. Bennett, "Privacy impact assessments in Canada", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

Companies might also be afraid a competitor might find out something from a PIA that could disadvantage the company that undertook the PIA.

We think such fears are over-wrought and misplaced. The Google Street View PIA report and the redacted enhanced driver's licence PIA, both reviewed in this deliverable, are evidence that organisations can survive and benefit from undertaking a PIA. Benefits of PIA are identified in the conclusions to this report.

PIA reports are not so easy to find. This is unfortunate for many reasons. Publication of a PIA report can show that an organisation is serious about privacy. It can help get feedback from stakeholders. PIA reports have educational value. Assessors and project managers can learn from the experience of others.

1.5 LEGAL BASES

In each of the country chapters of this report, we provide a review of the legal bases and guidance material for PIA. In each of those sections, we identify both fundamental rights protection instruments and the regulatory framework for privacy and data protection. We look at PIA-like activities already in force, i.e., these tools that share some features with basic PIA, such as prior checking (of a proposed processing operations) or prior consultation (of proposed legislation, data matching programme, etc.). A common denominator is ex ante examination. We list and briefly comment upon explicit PIA legal bases, in particular situations where an impact assessment is mandated by hard law. Relevant legal quotations and references are included. We also list PIA guidance material and look at proposals for PIA introduction, if any. Finally, a few legal observations are included in the conclusions to this report.

The legal bases of PIA found in the country chapters draw on, inter alia, a 2006 report by Privacy International, a 2007 study on PIA application and effects, commissioned by the UK Information Commissioner's Office, and PIAw@tch, an online PIA database launched in 2011.

* * *

The consortium is pleased to say that it has delivered somewhat more than it promised in this first phase of the PIAF project. We undertook to provide a review of the principal PIA methodologies in Australia, Canada, Hong Kong, New Zealand, the UK and US, and that has been done. However, we have also included a review of the Victoria Privacy Commissioner's PIA guide, the Ontario and Alberta PIA guides, and the DHS PIA guide. We have also reviewed and included comments on PIA audits by the Privacy Commissioner of Canada and the Government Accountability Office (GAO) in the US. In addition, we have included a review of the Irish PIA guide for health services.

We have delivered more than we promised in the interests of bringing to the attention of European policy-makers and data protection authorities additional information which we trust will be helpful in their consideration of an optimised PIA policy and practice. There are, in our view, good elements in these additional methodologies that can contribute to the development of an optimised PIA policy and practice in Europe. These are highlighted in the conclusion to this report.

2 AUSTRALIA

2.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

In this chapter, we present an analytical summary of the two best PIA methodologies in Australia, i.e., that produced by the Australian Privacy Commissioner in May 2010 and that produced by the Victoria Privacy Commissioner in April 2009. The chapter includes the legal basis for PIA in Australia, comments by PIA experts (notably PIA pioneer Roger Clarke) as well as a list of the best elements.

2.1.1 The Australian Privacy Commissioner (OPC) PIA Guide

The Office of the Privacy Commissioner (OPC) published its *Privacy Impact Assessment Guide* in August 2006, and a revised version in May 2010.[1] The Guide was based on considerable research into the experiences of and guidance provided in other jurisdictions, particularly New Zealand, Canada and Ontario, and on experience within Australia.[2] At 92 pages, it is one of the longer PIA guides, about the same length as the UK Information Commissioner's Office's *PIA Handbook*. A few months later, in November 2010, the OPC was subsumed into the Office of the Australian Information Commissioner (OAIC). The *PIA Guide* could be downloaded from the home page of the OPC, but now one has to cycle through a few pages of the OAIC website before finding the Guide.

The Guide has five main sections as well as seven "Modules" and an Appendix. The main body of the report is only 19 pages long, so the modules, which relate to points raised in the main body, account for the bulk of the guide. Following the Introduction, there is an overview of PIA, which covers what is a PIA, when a PIA will be important, who does the PIA, consultation and transparency, is a PIA necessary and threshold assessment. The next section covers the key stages and planning. And the one after, entitled "Doing the PIA", contains subsections on project description, mapping information flows and privacy framework, privacy impact analysis, privacy management, recommendations and the role of the Privacy Commissioner. The attached modules cover threshold assessment, nature of the project, mapping information flows, privacy impact analysis, compliance checklist for agencies, compliance checklist for organisations and privacy management.

Many PIA guidance documents contain a set of questions to stimulate consideration of a wide range of issues that should be addressed in a privacy impact assessment. This is also true of the Australian *PIA Guide*, which is noteworthy for the large number of questions which can be found in the modules.

The appendix has a list references, including the PIA guidance documents in Canada, New Zealand, the UK and US as well as Victoria state (see below). It also has a list of examples of actual PIA reports or summaries. No other PIA guidance document cites actual PIA reports.

The *Guide* is addressed to those who undertake a PIA, no matter whether they are from government agencies, the private sector or not-for-profit sector (i.e., civil society

[1] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, Sydney, NSW, August 2006, revised May 2010. http://www.privacy.gov.au. The *PIA Guide* can also be downloaded from http://www.oaic.gov.au/publications/guidelines.html#privacy_guidelines.

[2] Clarke, Roger, "Privacy Impact Assessment in Australian Contexts", *Murdoch eLaw Journal*, Vol. 15, No. 1, June 2008, pp. 72-93 [p. 84]. https://elaw.murdoch.edu.au/archives/elaw-15-1-2008.html

organisations). This is an important point to note. Most other PIA guidance documents are aimed at government agencies, but the Australian Guide obviously thinks that any organisation, from whatever sector, should undertake a PIA if it is planning a project that might pose risks to privacy. However, there is no legislative requirement in Australia to conduct a PIA. It notes (p. v) that the Privacy Act neither refers to PIAs nor requires organisations to do one. It does not impose a particular PIA style ("There is no one-size-fits-all PIA model.") but suggests a flexible approach depending on the nature of the project and the information collected. Module B gives some guidance and examples about how the PIA process can differ depending on the type of project or the stage.

Another important distinction between the Australian PIA Guide and some of its counterparts is that it makes the point (at p. iii) that information privacy is only one aspect of privacy. Other types of privacy include bodily privacy, territorial privacy and communications privacy.[3]

In the following pages, we paraphrase some of the key points from the Guide.

It defines a project as "any proposal, review, system, database, program, application, service or initiative that includes handling of personal information". The ICO *PIA Handbook* uses a similar definition. Note that the definition excludes proposed policies or legislation.

It defines (p. iv) a PIA as "an assessment tool that 'tells the story' of a project from a privacy perspective", and cites David Flaherty, Information and Privacy Commissioner of British Columbia from 1993 to 1999, as the source of this definition. Among other things, it says a PIA encourages good privacy practice and underpins good public policy in the project or, in the private sector, feeds into good risk management.[4]

It cites three main **risks** to an organisation in not handling privacy issues properly:

- Non-compliance with the letter or the spirit of relevant privacy law – leading to a privacy breach and/or negative publicity.
- Public concern and/or loss of credibility: A perceived loss of privacy or failure to meet expectations about how personal information will be protected, which may result in damage to brand reputation.
- System redesign: An adjustment to the project (at considerable expense and often late in the development stage).

Conversely, it sees three main **benefits of undertaking a PIA**:

- A PIA helps to avoid costly or embarrassing privacy mistakes.
- A PIA can help identify what needs to be done to ensure that a project complies with privacy law and other legislative requirements.
- A PIA gives an organisation the opportunity to consider the values the community places on privacy – trust, respect, individual autonomy and accountability – and to reflect those values in the project. A PIA also gives the organisation the opportunity to assess the project against its own values or business rules.

[3] Roger Clarke distinguished these different types some years ago. See Clarke, Roger, "What's privacy?", 2006. http://www.rogerclarke.com/DV/Privacy.html

[4] The *Australian/New Zealand Risk Management Standard* (AS/NZS 4360:2004) and the companion handbook *Risk Management Guidelines* (HB 436:2004) are used in government to assist in the process of assessing and managing project risks.

It sees other benefits too (p. viii), one of which is improving the project's consultation process. Thus, it regards consultation with external stakeholders, including the public, as an element in good PIA practice, as a way to more comprehensively identify privacy issues and to ensure stakeholders are better informed about the project's privacy and information handling aspects.

The *PIA Guide* says (p. viii) a PIA should be an integral part of the project from the beginning. A PIA should evolve with and help shape the project, which will help ensure that privacy is "built in" rather than "bolted on" (which echoes the same wording used in the ICO *PIA Handbook*).

Who does the PIA?

According to the *PIA Guide* (pp. ix-x), the project manager must decide if a PIA is necessary or desirable. Generally, a PIA makes use of various "in-house experts" and outside expertise as necessary. The Guide suggests that if a project has significant privacy impacts, a robust and independent PIA conducted by external assessors may be preferable.[5] "An independent assessment may help the organisation to develop community trust in the PIA findings and the project's intent."[6]

Consultation and transparency

The *PIA Guide* says (p. x) that "Consultation with key stakeholders is basic to the PIA process."

> A PIA should always consider community privacy attitudes and expectations. Affected individuals are likely to be key stakeholders, so wider public consultation is important, particularly where a lot of personal information is being handled or where sensitive information is involved. Public consultation also adds to community awareness about the project and can increase confidence in the way the project (and the organisation) is handling personal information.

The Privacy Commission encourages organisations, "where appropriate", to make the PIA findings available to the public (p. xviii).[7] The PIA Guide says (p. x) publication "adds value; demonstrates to stakeholders and the community that the project has undergone critical privacy analysis; contributes to the transparency of the project's development and intent".

The *PIA Guide* thus distinguishes itself from most other guidance documents on these two key points, i.e., stakeholder engagement and publication. The ICO *PIA Handbook* also emphasises consultation with external stakeholders, but most others do not. The *PIA Guide*

[5] Although the Privacy Commissioner's Office says it does not endorse particular assessors, the *PIA Guide* helpfully provides a link to its webpage (www.privacy.gov.au/aboutprivacy/helpme/psp) listing some assessors, the only guidance document to do so.

[6] However, if the external assessor is paid by the project manager, one could call into question how truly independent the assessor can be. John Edwards and Nigel Waters in their chapters both draw attention to this problem in Wright, David, and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 (forthcoming).

[7] The Privacy Commissioner acknowledges (p. xviii) that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part. However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the Commissioner encourages organisations to consider the release of a summary version.

advocates publication of PIAs, which is what US government agencies are supposed to do too, but most other guidance documents do not advocate publication (in Canada, government agencies are supposed to publish summaries, but are not obliged to publish the full PIA report).

Thus, the Australian *PIA Guide* sets a new benchmark for PIA on consultation and transparency.

Is a PIA necessary?

The first question to ask when assessing whether a PIA is needed is: "Will any personal information be collected, used or disclosed in the project?" The Guide provides a *threshold assessment* (see Module A) that helps the assessor (or project manager) to decide whether the project needs a PIA.

Module A notes that there is no hard-and-fast rule about when to do a PIA, that each project must be considered individually. The threshold assessment establishes whether the project collects, uses or discloses personal information. Generally, if personal information is not involved in the project, the project is unlikely to impact on information privacy and a PIA will not be necessary. However, says the PIA Guide (p. xx), just because there is no personal information collection in a project does not guarantee that there will be no information privacy impact. It goes on to explain that personal information does not always have to include details such as an individual's name. It may include other information that can identify an individual or allow their identity to be worked out. It gives an example: Generic information about ethnic origin may not, by itself, identify an individual. But if ethnicity and other information is disclosed about an individual in a small town (that has only a limited number of people from that ethnic background), the person could be identified and the information could become personal information under the Privacy Act.

Key stages to the PIA process

Although the PIA Guide acknowledges different PIA models, it says (p. xii et seq.) there are generally five key stages in the PIA process:

(1) *Project description*

A PIA should include a broad, "big picture" description of the project, including:
- The project's overall aims.
- How these aims fit with the organisation's broader objectives.
- The project's scope and extent.
- Any links with existing programs or other projects.
- The key privacy elements, e.g., the extent and type of information to be collected, how security and data quality will be addressed, and how the information will be used and disclosed.

(2) *Mapping the information flows and privacy framework*

A PIA should describe and map the project's personal information flows and document all relevant legislative and organisational rules. Detailed information mapping should include:
- what personal information will be handled

- how the personal information will be collected
- how it will be used
- internal flows
- disclosures
- security measures
- data quality measures
- any privacy, secrecy or other relevant legislation applying to the information flow
- any organisational or other business privacy rules applying to the information flow.

Once the mapping is done, the assessor can begin an assessment of privacy impact or compliance issues and how they could be addressed, including:
- the way personal information is collected, used and disclosed
- the way individuals can access information about them, and correct it if necessary
- security safeguards
- the processes for ensuring data quality
- whether an identity management system is involved.

Module C gives a picture of information flows to help identify and assess possible privacy issues.

(3) *Privacy impact analysis*

At this stage, the PIA should identify and critically analyse how the project impacts upon privacy, positively and negatively, whether the impacts are necessary or avoidable and whether the project has unacceptable privacy impacts. A stakeholder or public consultation will help in working out how to improve the privacy outcomes. Module D has various questions to help the assessor perform a privacy impact analysis. It says privacy impact analysis investigates:
- how information flows affect individuals' choices in the way personal information about them is handled
- the degree of intrusiveness into individuals' lives
- compliance with privacy law
- how the project fits into community expectations.

Modules E and F ask about compliance issues in relation to the Privacy Act principles. Module E is for government agencies, while Module F is for private sector and not-for profit organisations.

There are two sets of similar principles – the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) – which appear in the Privacy Act and which are subject to a set of questions in Modules E and F. The IPPs, referenced in Module E, regulate how Australian and ACT government agencies manage personal information, including its collection, record keeping, use, disclosure, storage and security. The IPPs also allow individuals to access personal information about them and have it corrected if it is wrong. Under the Privacy Act, agencies must ensure that a service provider with whom they contract does not breach the IPPs nor the NPPs. Four NPPs have no IPP equivalents. The National Privacy Principles (NPPs), referenced in Module F, regulate how organisations (including all private sector health organisation and some small businesses) must manage personal information, including collection, use and disclosure, quality and security, openness, access and correction, identifiers, anonymity, transborder data flows and sensitive information.

(4) *Privacy management*

The PIA should identify options to get rid of or lessen any negative privacy impacts. The PIA Guide assures the project manager "This does not necessarily mean compromising your organisation's goals. You may find options that will make a significant difference to the privacy impact and still allow you to achieve the project's goals."

(5) *Recommendations*

The final PIA report should identify avoidable impacts or risks and recommend ways to remove them or reduce them to an acceptable level.

The *PIA Guide* says (p. xviii) the PIA should feed into planning the project's next steps. This could include resource allocation (including training), stakeholder management, senior management briefing, designing, trialling, testing, consultation, public education and evaluation. As the project progresses, the PIA may need to be revisited to take account of developments in the design or implementation of the project.

Role of the privacy commissioner

The PIA Guide (p. xix) says the Office has no formal role in the development, endorsement or approval of PIAs. However, subject to available resources, the Office may be able to help organisations with advice during the PIA process.

Scope of the project

Module B helps the organisation decide on the most appropriate PIA process taking into account the project's scope, whether the project is new or an alteration of existing project and how advanced the project is.

The scope of the project is a function of attributes including:

- *Quantity* of the personal information handled.
- *Sensitivity* of the personal information involved, such as biometric or genetic components.
- *Significance* of the project – its size or complexity.
- *Interaction* – the degree of cross-organisation or cross-sector involvement such as in sharing or data-matching across organisations or jurisdictions.
- *Public impact* of the project, i.e., the extent to which it handles (processes) personal information about a "significant number" of individuals.

A project's privacy scope can increase depending on the risk of adverse privacy impacts. Generally, the greater the scope of the project, the more detailed the PIA will be.

Like the ICO *PIA Handbook*, which distinguishes between "small-scale" and "full-scale" PIAs, the Australian *PIA Guide* distinguishes between "short" and "comprehensive" PIAs (pp. xxvi-xxvii). Also, like the Handbook, the Guide says that even short PIAs should go through the same five stages as for a comprehensive PIA, but more briefly.

2.1.2 The Victorian Privacy Commissioner (OVPC) PIA Guide

Roger Clarke has described the PIA guide produced by the Office of the Victorian Privacy Commissioner (OVPC) as "one of the three most useful guidance documents available in any jurisdiction, anywhere in the world".[8] The OVPC guide actually consists of three documents, all of which are available on the OVPC website. The three documents are *Privacy Impact Assessments: A guide for the Victorian Public Sector* [hereafter referenced as the OVPC *PIA Guide*], an accompanying guide and a template.[9]

The current OVPC *PIA Guide* dates from April 2009. It is the second edition of the guide originally published in August 2004.[10] The OVPC *Guide* consists of an Introduction and several sections: What is a PIA?, Is a PIA needed for our project?, Why should a PIA be done?, When should a PIA be done?, Who should do the PIA?, Who else should be involved?, How is a PIA done?, What should be done next? as well as an appendix on threshold privacy assessment. The *Guide* is 28 pages long. The *Accompanying Guide* is another 26 pages, and the template is 63 pages in length.

The *Accompanying Guide* sets out various risks thematically linked to Victoria's privacy principles as well as possible strategies for mitigating those risks. The *Accompanying Guide* identifies risks relating to anonymity, data collection, use and disclosure of data, transborder data flows, data quality and security, disposal, access to data, correction of data, openness, accountability. It also sets out risks relating to other types of privacy in additional to informational privacy, i.e., bodily privacy, territorial privacy, locational privacy and communications privacy.

The template provides the structure of a PIA report, which the user can adapt to his or her circumstances. The template has been produced as a Word document for ease of use by the assessor.

As its title indicates, the OVPC *PIA Guide* is primarily aimed at the Victorian public sector. However, the Introduction adds (p. 2) that it may assist anyone undertaking a PIA. Like the Australian OPC *Guide*, it says that privacy considerations must be broader than just information privacy; bodily, territorial, locational and communications privacy must also be considered. The *Guide* says that, since its first edition, "PIAs are now more common in Australia and around the world" and that it has been able to draw on the experience of others to make the *Guide* more practical and effective.

The *Guide* describes (p. 4) a PIA (p. 4) as "a tool which should offer both a diagnosis of a project's well-being in terms of its privacy impacts, and a prescription of ideas to help treat any problems diagnosed".

The *Guide* uses (p. 5) the word "project" to encompass any type of proposed undertaking, be it "a project, process, system, legislation, program, service, database, application, initiative,

[8] Clarke, Roger, "PIAs in Australia: A work-in-progress report", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

[9] Office of the Victorian Privacy Commissioner (OVPC), *Privacy Impact Assessments: A guide for the Victorian Public Sector*, Edition 2; *Accompanying Guide – A guide to completing Parts 3 to 5 of your Privacy Impact Assessment Report*; *Privacy Impact Assessment Report template*. All three were published in April 2009 and can be found at http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/publication-types?opendocument&Subcategory=Guidelines&s=

[10] Helen Versey, the Victorian Privacy Commissioner, who has signed the Introduction, says the new edition of the PIA Guide has been revised by Anna Johnston of the consulting firm Salinger Privacy. Ms Johnston is the former New South Wales Deputy Privacy Commissioner.

policy or procedure". It explicitly mentions "legislation" and "policy", which are not mentioned in the Australian OPC *Guide*.

> The project need not be new; it might be a proposal to change an existing system or legislation, which might lead to new ways of handling personal information, or new data-sharing. Nor does the project need to be large; the size or budget for a project is not a useful indicator of its likely impact on privacy. The project does not even need to involve recorded "personal information" as defined under the Information Privacy Act; a program that may include the need for bodily searches can still impact on privacy even if no personal information is recorded, and therefore the right to privacy in the Charter of Human Rights and Responsibilities needs to be considered.

The Guide recommends that a simple **threshold privacy assessment** should be routinely conducted for every project. It defines a threshold privacy assessment as an initial consideration of a project, to determine whether a PIA is necessary. The Guide has an appendix with 17 simple yes/no questions (e.g., will the project involve the collection of personal information, compulsorily or otherwise?). If the answer to any of the questions is yes, the organisation should seriously consider initiating a PIA.

The Guide says (p. 6) up-front commitment from an organisation's executive to the conduct of PIAs is needed as the first step towards ensuring buy-in to the PIA's eventual recommendations.

Why do a PIA?

The Guide (p. 7 et seq.) offers several reasons why a PIA be done.

A Privacy Impact Assessment is often described as an "early warning system". It allows the organisation to detect potential privacy problems, take precautions and build tailored safeguards before, not after, it makes heavy investments.

The PIA affirms that privacy issues have been addressed and that reasonable steps have been taken to provide an adequate level of privacy protection at the time of assessment. The PIA also provides a mechanism for reviewing the privacy impact of projects as changes occur.

The primary objective of a PIA is to allow any negative privacy impact to be weighed properly against whatever benefits the project offers in the public interest.

Doing a PIA can demonstrate compliance in the context of a subsequent complaint, privacy audit or compliance investigation.

Implementing the PIA process demonstrates to employees and contractors that the organisation takes data protection seriously.

Benefits of PIA

The Guide cites several benefits of undertaking a PIA. It

- helps to ensure compliance with the Information Privacy Principles (IPPs) in the Information Privacy Act and the Charter of Human Rights and Responsibilities;
- assists in anticipating and responding to the public's privacy concerns;
- exposes any internal communication gaps or hidden assumptions about the project;

- promotes awareness and understanding of privacy issues;
- helps reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early;
- enhances informed decision-making; and
- enhances the legitimacy of a project, especially where some compromise or trade-off is necessary.

Risk management

The Victorian Government *Risk Management Framework* requires all department and agency heads to attest in their annual reports that they have risk management processes in place, consistent with the *Australian/New Zealand Standard AS/NZS 4360: 2004*, and that a responsible body or audit committee verifies that view. The *Guide* argues (p. 8) that PIAs should form part of the risk evaluation and management

Types of privacy

The *Guide* says that a PIA must consider all types of privacy, i.e.,
- bodily privacy (to protect the integrity of the physical person);
- territorial privacy (to protect personal space, objects and behaviour);
- communications privacy (to protect against eavesdropping);
- locational privacy (to protect against surveillance); and
- information privacy (to protect personal information).

Value to the public

The *Guide* says (p. 9) that a proper PIA can give the public confidence that their privacy has been adequately considered and addressed, that it can allay fears about loss of privacy or about protection of personal information. It can also assist in anticipating public reaction to the privacy implications of a given proposal.

The *Guide* advocates publication of the PIA report: Releasing a PIA Report gives the public an opportunity to express concerns and have them addressed before a project has been implemented.

When should a PIA be done?

The Guide says (p. 10) a PIA should be initiated at the early stages of project development and planning so that it can influence decision-making about the design of the project. The PIA should be dynamic, updated as changes are contemplated to projects.

It estimates that a "comprehensive" PIA on a significant or complex project may take between 20 and 60 business days to complete.

Who should do the PIA?

A PIA may be conducted "in-house" or by an external consultant. It foresees (p. 11) that some PIAs may involve more than one organisation, hence, a team may need to be assembled from each organisation. The nature and size of the project may determine whether an internal individual or team conducts the PIA, with or without external specialist advice.

The involvement of project or program managers is essential for the PIA process. They will need to supply the assessor with project and contextual documentation such as the business case, and to explain and answer questions about data flows, accountability and governance structures, and stakeholder relations.

A PIA may need to involve other internal staff, including:
- IT staff, to answer questions about data security, the project's technical architecture, network security, online applications, backup procedures and data flows;
- procurement officers, to ensure that privacy considerations are included in the drafting of tender documents as well as the evaluation of tender responses;
- records managers, to advise on how information is stored and disposed;
- facilities managers, to explain how physical security is managed;
- human resources managers, if the project will involve employee records;
- legal staff, to ensure the project can proceed lawfully and to examine any provisions dealing with secrecy, confidentiality or other restrictions on the collection, storage, use or disclosure of personal information.

The organisation should consult early with the privacy commissioner if
- there is a large amount of personal information at issue;
- the project involves sensitive information;
- there will be sharing of personal information between organisations;
- any personal information will be handled by a contracted service provider;
- any personal information will be transferred outside Victoria; or
- there is likely to be public concern about actual or perceived impact on privacy.

External stakeholders and public consultation

If a project involves more than one organisation, including contracted service providers or other third party services, the *Guide* advises (p. 13) that the PIA should consider the privacy risks arising from those organisations too.

The *Guide* says that public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence amongst the public that their privacy has been considered. Public consultation may generate new options or ideas for dealing with a policy problem.

Like most other guidance documents, the OVPC *PIA Guide* says that a PIA should assess not only a project's strict compliance with privacy and related laws, but also public concerns about the wider implications of the project.

The *Guide* identifies (p. 14) factors influencing the decision to undertake a public consultation:
- there is likely to be public concern about actual or perceived impact on privacy;
- the project may affect the privacy of a large number of people or of vulnerable groups;
- the project may need formal authority for the collection and handling of personal information;
- the organisation may see a need to build trust in a new practice or technology.

The *Guide* cites the UK ICO with regard to the benefits of undertaking a consultation.

It says that if wide public consultation is not an option, the organisation could consult key stakeholders who represent the project's client base or the wider public interest or who have expertise in privacy, human rights and civil liberties.

It cites the New Zealand *PIA Handb*ook which notes that "Proposals may be subject to public criticism even where the requirements of the Act have been met. If people perceive their privacy is seriously at risk, they are unlikely to be satisfied by (an organisation) which justifies its actions merely by pointing out that technically it has not breached the law."[11]

The PIA report

The OVPC has developed a template for a PIA report. The *Guide* says (p. 16) the PIA report should work as a stand-alone document, which provides the lay reader with a description of the project's objectives, drivers, scope, environment, and operational details. The report should map the data flows, including:

- collection (the type of personal information collected, the original source of the information, and the circumstances for collection);
- use (the processing of the information, and its intended uses);
- disclosure (to whom the information will be distributed, for what purposes or in what circumstances);
- data quality (how the quality of personal information will be assured);
- data security (the safeguards that will operate against misuse, loss, unauthorised access, modification or disclosure, including at disposal); and
- access and correction (how individuals will be able to access and, if necessary, correct their personal information).

Data flow diagrams should show each business unit and organisation involved in the project, including contracted service providers and other jurisdictions, and show how personal information will move between those units.

The Template PIA Report's Accompanying Guide lists common risks associated with each IPP, and the other dimensions to privacy.

Mitigating the risks

The *Guide* offers (p. 18) a few basic strategies for mitigating privacy risks:

- ensure the project has a sound justification with a public benefit;
- minimise the personal information collected to only what is absolutely necessary;
- maximise transparency about what personal information will be collected, stored, used and disclosed;
- limit uses and disclosures of the information; and
- protect data security.

Recommendations to mitigate privacy risks can relate to:

- IT design;
- legislation;
- policies and procedures;

[11] Office of the Privacy Commissioner (New Zealand), Privacy Impact Assessment Handbook, June 2007, p.24

- transparency (internal and/or external communication);
- staff training; and
- accountability measures.

The PIA report should identify which privacy risks cannot be mitigated, the likely public reaction to such risks, and whether the risks are outweighed by the public benefit in the project proceeding nonetheless.

Follow-up

Following completion of the PIA report, the organisation will need to make decisions about the PIA report's recommendations. It might add the significant risks identified in the PIA to the organisation's risk register. The organisation will need to consider how residual risks will be managed, who will be accountable for future privacy management of the project, when and how the PIA will be updated and reviewed.

Publishing the report

The report generally recommends (p. 20) publication of the report, but recognises some considerations, such as security, may influence the decision to publish. In such cases, it says that a properly edited PIA report will usually suffice to balance the security and transparency interests. One option is to publish both the PIA report and the organisation's response to its recommendations, and then seek feedback through consultation on whether the proposed response is acceptable to stakeholders, whether the project should proceed, or which option/s to follow.

It encourages organisations to send a copy of the PIA report to the OVPC.

2.2 LEGAL BASIS

2.2.1 Australia – federal level

1. General framework for privacy and data protection

Despite some calls,[12] there is no general fundamental rights protection instrument on the federal level in Australia. Yet a few states/territories enacted such laws (see *infra*). The Australian Human Rights Commission,[13] established in 1986, has statutory responsibilities under certain substantive federal anti-discrimination and human rights laws, e.g. the Racial Discrimination Act 1975 and Age Discrimination Act 2004.

The general privacy and data protection legal framework in Australia on the federal level is based principally of the **Privacy Act 1988** (Cth.)[14] dealing with informational privacy. It came into effect on 1 January 1989. Sec. 14 contains Information Privacy Principles (IPPs), binding both the Commonwealth and the Australian Capital Territory public sector. The Act

[12] Amnesty International, *Government fails to implement a Human Rights Act*, 21 April 2010. http://www.amnesty.org.au/news/comments/22903

[13] Australian Human Rights Commission. http://www.hreoc.gov.au

[14] Privacy Act 1988 (Cth.), Act No. 119 of 1988. http://www.comlaw.gov.au/Details/C2011C00503 (official source).

was amended substantially by the **Privacy Amendment (Private Sector) Act 2000** (Cth.) to cover the private sector too.[15] Sec. 139 added the Schedule 3 on the ten National Privacy Principles (NPPs) to the Privacy Act 1988. The Australian Information Commissioner (OAIC)[16] was established under the Australian Information Commissioner Act 2010 (Cth.).[17]

2. Laws on PIA forerunners

Two provisions of the Privacy Act 1988 share some characteristics with **prior consultation**. Sec. 27(1) states that one of the functions of the Information Commissioner is:

> (b) to examine (with or without a request from a Minister or a Norfolk Island Minister) a proposed enactment that would require or authorise acts or practices of an agency or organisation that might, in the absence of the enactment, be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals and to ensure that any adverse effects of such proposed enactment on the privacy of individuals are minimised;

This provision is further explained in Sec. 31:

> (1) Where the Commissioner has examined a proposed enactment under paragraph 27(1)(b), subsections (2) and (3) of this section have effect.
> (2) If the Commissioner thinks that the proposed enactment would require or authorise acts or practices of an agency or organisation that would be interferences with the privacy of individuals, the Commissioner shall:
> (a) report to the Minister about the proposed enactment; and
> (b) include in the report any recommendations he or she wishes to make for amendment of the proposed enactment to ensure that it would not require or authorise such acts or practices.
> (3) Otherwise, the Commissioner may report to the Minister about the proposed enactment, and shall do so if so directed by the Minister.

Similar powers are vested in the Information Commissioner with regard to data matching[18] [Sec. 27(1)]:

> (k) to examine (with or without a request from a Minister or a Norfolk Island Minister) a proposal for data matching or data linkage that may involve an interference with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals and to ensure that any adverse effects of such proposal on the privacy of individuals are minimised

The Data-matching Program (Assistance and Tax) Act 1990 (Cth.) deals with this issue in detail.[19]

---

[15] Clarke, Roger, "Privacy Impact Assessment in Australian Contexts," 2008. http://www.rogerclarke.com/DV/PIAAust.html#PPA

[16] Office of the Australian Information Commissioner, http://www.oaic.gov.au

[17] Australian Information Commissioner Act 2010 (Cth.), Act No. 52 of 2010. http://www.comlaw.gov.au/Details/C2010A00052

[18] As the OAIC explains: "Data-matching involves bringing together data from different sources and comparing it.… For example, records from different departments are often compared to identify people who are being paid benefits to which they are not entitled or people who are not paying the right amount of tax. Data-matching poses a particular threat to personal privacy because it involves analysing information about large numbers of people without prior cause for suspicion." Cf. http://www.privacy.gov.au/law/other/datamatch

[19] Data-matching Program (Assistance and Tax) Act 1990 (Cth.), Act No. 20 of 1991. http://www.comlaw.gov.au/Details/C2011C00477

3. PIA legal bases

There is no explicit basis for PIA in the laws of Australia.

In the by-laws of the Biometrics Institute, its Privacy Code (2006)[20] explicitly requires PIA be conducted:

> 13.4. A Code Subscriber shall conduct privacy impact assessments as part of the planning and management process for biometrics implementation.

Pursuant to Sec. 18BB(2) of the Privacy Act 1988 (Cth.), this Code has been approved by the (then) Privacy Commissioner on 19 July 2006.

4. Guidance material

Various public bodies have issued some guidance material:

- Office of the Privacy Commissioner (now OAIC, see *supra*)
  - *The use of data matching in Commonwealth administration – Guidelines* (February 1998)[21]
  - *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals* (21 December 2001),[22] of which Guideline 3 recommends that "agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI system"[23]
  - *Privacy Impact Assessment Guide* (August 2006,[24] revised May 2010),[25] which is considered a basic PIA guidance material in Australia
- Medicare Australia: *Privacy Impact Assessment (PIA) – Increased MBS* [Medicare Benefits Schedule] *Compliance Audits* (28 April 2009)[26]
- Department of Defence: *Defence Privacy Impact Checklist*, February 1998.[27]

Among private bodies, La Trobe University has issued a *Privacy Impact Assessment (PIA) Guide – Human Ethics Applications*, 10 December 2005.[28]

---

[20] Biometrics Institute, *Privacy Code*, 2006. http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8

[21] Office of the Privacy Commissioner, *The use of data matching in Commonwealth administration – Guidelines,* 1998. http://www.privacy.gov.au/materials/types/download/8688/6527

[22] Office of the Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals*, 2001, http://www.rogerclarke.com/DV/OAPC-2001.pdf

[23] Clarke explains that "Public Key Infrastructure (PKI) is the means whereby digital signature schemes are delivered." Cf. http://www.rogerclarke.com/DV/PIAAust.html#PIAA

[24] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006. http://www.privacy.gov.au/materials/types/download/9349/6590

[25] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, May 2010. http://www.privacy.gov.au/materials/types/download/9509/6590

[26] Medicare Australia, *Privacy Impact Assessment (PIA) – Increased MBS Compliance Audits*, 2009. http://www.health.gov.au/internet/main/publishing.nsf/Content/C010759A8FB2E35DCA25759300011241/$File/Privacy%20Impact%20Assessment%20for%20the%20IMCA%20initiative.pdf

[27] Department of Defence, *Defence Privacy Impact Checklist*, 1998. http://www.defence.gov.au/fr/Privacy/defence-piachecklist-Feb08.doc

[28] La Trobe University, *Privacy Impact Assessment (PIA) Guide Human Ethics Applications. An assessment tool to identify risks with respect to the privacy of research participants*, 2005. http://www.latrobe.edu.au/privacy/assets/downloads/pia_human_ethics_applications.pdf

5. Proposals

In 2003, the (then) Federal Privacy Commissioner submitted to the Parliament's Joint Committee of Public Accounts and Audit a set of recommendation stating that:[29]

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

In 2005, the Legal and Constitutional References Committee of the Australian Senate recommended:[30]

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

In 2007, the Australian Law Reform Commission (ALRC) recommended that:[31]

> 44.70 … PIAs should be given some legislative underpinning in the Privacy Act. This could be done by either:
> - amending the Privacy Act to include a requirement to prepare a PIA for proposed projects and developments that significantly impact on the handling of personal information; or
> - encouraging the preparation of PIAs and empowering the Commissioner to direct the preparation of a PIA where the Commissioner thinks a project or development is likely to have a significant impact on the handling of personal information.

Further, the ALRC called for PIA introduction in recommendations 47-4 and 47-5:[32]

> 4. The Privacy Act should be amended to empower the Privacy Commissioner to:
> (a) direct an agency to provide to the Privacy Commissioner a Privacy Impact Assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and
> (b) report to the ministers responsible for the agency and for administering the Privacy Act on the agency's failure to comply with such a direction.

---

[29] Office of the Federal Privacy Commissioner, *Management and Integrity of Electronic Information in the Commonwealth. Submission*, 2003, p. 20, http://www.privacy.gov.au/materials/types/download/8759/6570

[30] The [Australian] Senate, Legal and Constitutional References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005.
http://www.aph.gov.au/senate/committee/legcon_ctte/completed_inquiries/2004-07/privacy/report/report.pdf

[31] Australian Law Reform Commission *ALRC Discussion Paper 72. Review of Australian Privacy Law*. 2007.
http://www.austlii.edu.au/au/other/alrc/publications/dp/72/44.html

[32] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice, Report 108*, 2007. http://www.austlii.edu.au/cgi-bin/sinodisp/au/other/alrc/publications/reports/108/_3.html. Further information can be obtained at http://www.privacy.gov.au/law/reform

5. The Office of the Privacy Commissioner should develop and publish Privacy Impact Assessment Guidelines tailored to the needs of organisations. A review should be undertaken in five years from the commencement of the amended Privacy Act to assess whether the power in Recommendation 47–4 should be extended to include organisations.

2.2.2 Victoria state

1. General framework for privacy and data protection

The basic fundamental rights instrument in Victoria is the Charter of Human Rights and Responsibilities Act 2006 (Vic).

The general privacy and data protection legal framework in the Australian State of Victoria consists of the **Information Privacy Act 2000** (Vic.).[33] It came into effect on 1 September 2002. The **Health Records Act 2001** (Vic.), which came into effect on 1 July 2002, regulates the health information in Victoria separately.[34] Sec. 19 contains the Health Privacy Principles. The former Act created the Victorian Privacy Commissioner [Sec. 50(1)][35] and the latter – the Health Services Commissioner (Sec. 87).

2. Laws on PIA forerunners

The following are the functions of the Victorian Privacy Commissioner with regard to **prior consultation** [Sec. 58 of the Information Privacy Act 2000 (Vic.)]:

(l) to examine and assess any proposed legislation that would require or authorise acts or practices of an organisation that may, in the absence of the legislation, be interferences with the privacy of an individual or that may otherwise have an adverse effect on the privacy of an individual, and to report to the Minister the results of the examination and assessment;
(n) to make reports and recommendations to the Minister, or the Minister responsible for a public sector agency or a Council administering a public register, in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of personal privacy;
(t) to examine and assess (with or without a request) the impact on personal privacy of any act or practice, or proposed act or practice, of an organisation;

Similarly, the Health Service Commissioner is empowered [Sec. 87 of the Information Privacy Act 2000 (Vic.)] with **prior consultation** functions:

(p) to examine and assess (with or without a request) the impact on personal privacy of any act or practice, or proposed act or practice, of an organisation;

3. PIA legal bases

No explicit basis for PIA in the laws of Victoria has been found.

4. Guidance material

[33] Information Privacy Act 2000 (Vic.), Act No. 98 of 2000.
http://www.austlii.edu.au/au/legis/vic/consol%5fact/ipa2000231/index.html
[34] Health Records Act 2001 (Vic.), Act No. 2 of 2001.
http://www.austlii.edu.au/au/legis/vic/consol%5fact/hra2001144/index.html
[35] Office of the Victorian Privacy Commissioner. http://www.privacy.vic.gov.au

The Office of the Victorian Privacy Commissioner issued a PIA guide in August 2004[36] and revised in April 2009.[37] A template and the Accompanying Guide support it.[38] A guide on data-matching[39] complements the privacy guidance material in Victoria.

2.3 COMMENTS ON THE SHORTCOMINGS AND EFFICACY OF PIA IN AUSTRALIA BY PIA EXPERTS

Australian privacy expert Roger Clarke notes that under the current statutory regime, the performance of a PIA is not mandatory.[40] However, he remarks that the Privacy Commissioner's communications with agencies and the private sector in relation to schemes that have privacy implications routinely encourage that a privacy impact assessment be undertaken. He reports that during the first year after it was published, the PIA Guide had attracted 23,000 hits and downloads. On the other hand, he adds, "PIAs are not yet performed as a matter of course, even within Government, even for projects with significantly privacy-invasive features."[41]

He describes the scope of PIAs as "much more than an audit of compliance with the law", that the activity needs "to address all dimensions of privacy". He describes consultation as central to the process and, citing one of his earlier articles, says: "The objectives of a PIA cannot be achieved if the process is undertaken behind closed doors. In a complex project applying powerful technologies, there are many segments of the population that are affected. It is intrinsic to the process that members of the public provide input to the assessment, and that the outcomes reflect their concerns."[42]

Clarke says the lightly-revised version of the Australian Privacy Commissioner's PIA Guide published in 2010 "was intended to be more obviously applicable to the private sector as well as government agencies", that it "is process-oriented and practical, and indicates the need for broad scope". However, he finds that it has some weaknesses: "Although it recognises the significance of the views of the affected public, it fails to provide clear advice on how to treat

[36] Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments – a guide*. August 2004. http://www.rogerclarke.com/DV/OVPC-2004.pdf

[37] Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments. A guide for the Victorian Public Sector,* Ed. 2, April 2009. http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide/$file/guideline_05_09_no1.pdf

[38] Office of the Victorian Privacy Commissioner, *Accompanying Guide. A guide to completing Parts 3 to 5 of your Privacy Impact Assessment Report*, 2009. http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-report-accompanying-guide/$file/guideline_05_09_no2.pdf. *PIA Template*. http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessment-report-template

[39] Office of the Victorian Privacy Commissioner, *Data Matching in the Public Interest, A guide for the Victorian public sector*, Ed. 1, August 2009. http://www.privacy.vic.gov.au/privacy/web2.nsf/files/data-matching-in-the-public-interest-a-guide/$file/guideline_08_09_no1.pdf

[40] However, Clarke (2008, p. 86) says a Senate committee did recommend in 2005 that "the Privacy Act be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information."

[41] Clarke, 2008, pp. 84-85.

[42] Clarke Roger, "PIAs in Australia: A work-in-progress report", in Wright, David, and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming]. Clarke cites his earlier article: "Privacy Impact Assessment Guidelines", Xamax Consultancy Pty Ltd, February 1998. http://www.xamax.com.au/DV/PIA.html

them as stakeholders, lacks practical advice on consultation processes and fails to mention advocacy groups as a means of gaining an appreciation of the views of the relevant public."[43]

During the decade following 2000, there was considerable unrest among consumers about electronic marketing practices. Consultative processes conducted by the Department of Communications resulted in regulation firstly of unsolicited e-mail by the Spam Act 2003, and, secondly, of unsolicited tele-marketing calls by the Do Not Call Register Act 2006. The Do Not Call Register attracted more than 200,000 registrations in the first 24 hours it was open, passed 2 million registrations within the first six months, and stood at 5 million in mid-2010, even though the law exempts categories of organisations widely regarded as abusing the medium, including charities, researchers and politicians.

In the telecommunications sector more generally, the Telecommunications Act and the Telecommunications (Interception and Access) Act include provisions relating to security and privacy. The privacy-protective aspects of these laws are used more effectively by the Telecommunications Industry Ombudsman (TIO) and the Australian Communications and Media Authority (ACMA) than the provisions of the Privacy Act are by the Privacy Commissioner.[44]

Clarke comments that "It is entirely feasible to interpret the Guide as requiring an assessment of broad scope, and some PIAs conducted using it have extended beyond information privacy, and beyond extant data protection law. Unfortunately, narrow interpretations are also possible, and some agencies have performed what they have called PIAs, but which were no more than checks of compliance with the Information Privacy Principles."

Among his other concerns are that the document is not as easy to find on the OAPC's website as is desirable.[45]

Although the importance of stakeholder engagement is presented at some length, consultation is entirely omitted from the description of the PIA process. The orientation is strongly towards impacts and issues, with far less attention paid to solutions and avoidance and no mention at all of mitigation. In addition, the Office has compromised its position on several occasions, both by participating directly in PIA projects conducted by particular agencies and by failing to convince those agencies to effectively engage with the affected public.[46]

On the other hand, Clarke describes the Victorian PIA Guide as "comprehensive, extending beyond legal requirements to encompass public concerns and implications for all dimensions of privacy. It stresses the importance of public consultation. It adopts a checklist approach, but the checklists incorporate advice on the process needed to satisfy the requirement." Furthermore, he says that the Victorian Privacy Commissioner "has communicated the existence of the PIA guidelines through its network of privacy officers in government

[43] Clarke, 2012.
[44] Cyberspace Law and Policy Centre of the University of New South Wales, "Communications privacy complaints: In search of the right path", A consumer research report supported by the Australian Communications Consumer Action Network (ACCAN), Sydney, September 2010.
http://www.cyberlawcentre.org/privacy/ACCAN_Complaints_Report/report.pdf. Cited in Clarke, 2012.
[45] Clarke, 2012.
[46] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, February 2011, pp. 111-120 [p. 118].
http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full or
http://www.rogerclarke.com/DV/PIAG-Eval.html

agencies, conducted training sessions and mentioned the PIA guidelines in various presentations."

Clarke says one weakness of the Victorian Guide is that "it would be feasible for an agency to interpret a PIA as being a report, rather than as a process. In addition, the Guide contemplates the possibility of a PIA being conducted by an independent organisation such as a consultancy. This would have the effect of shielding the agency from the relevant public, and prevent assimilation of information by the agency's executives and staff. The Guide lacks visibility in the health care sector, which is subject to a separate Commissioner who appears to place no emphasis on PIAs."

> On the other hand, the Template and the Accompanying Guide draw the assessor well beyond mere legal compliance, place considerable emphasis on consultation and solution-orientation, and provide instruction without permitting the assessor to abandon intellectual engagement with the work. The Guide's comprehensiveness, quality and practicality are all high, and it represents one of the three most useful guidance documents available in any jurisdiction, anywhere in the world, along with those produced by the UK Information Commissioner's Office (ICO) and the Ontario government.[47]

The revised version has one disadvantage in that it structures and describes the PIA process in terms of the preparation of the PIA Report—which risks readers thinking of a PIA as a mere product rather than primarily a process. On the other hand, the Template and the Accompanying Guide draw the assessor well beyond mere legal compliance, place considerable emphasis on consultation and solution orientation, and provide instruction without permitting the assessor to abandon intellectual engagement with the work. The Guide accordingly scores very highly against the criteria.[48]

Nigel Waters, PIA consultant and former Deputy Privacy Commissioner, notes the growing use of privacy impact assessment techniques, "although depressingly few of the initiatives are as transparent as they need to be, with limited opportunities for public consultation and debate".[49]

2.4 BEST ELEMENTS

The elements of the Australian PIA Guide that we most like and would recommend for a European PIA guidance include the following:

- It is aimed at government agencies, private sector and non-private (civil society) sector – i.e., any organisation impacting privacy should carry out a PIA for any new project.
- It makes the point that information privacy is only one type of privacy. A PIA could also address other types of privacy, namely, bodily, territorial and communications privacy.
- It has a list of the risks to an organisation in not handling privacy issues properly and benefits of carrying out a PIA.
- It says a PIA should be started early, so that it can evolve with and help shape the project, so that privacy is "built in" rather than "bolted on".
- It encourages organisations to consult with stakeholders. "Consultation with key stakeholders is basic to the PIA process."

[47] Clarke, 2012.
[48] Clarke, 2011, p. 119.
[49] Waters, Nigel, "Who am I?", A Paper for [Id]entity 08, a conference organised by the Office of the Victorian Privacy Commissioner, Melbourne, 12 Nov 2008. http://www.austlii.edu.au/au/journals/ALRS/2008/12.html

- Although it does not "impose" a particular PIA model, it identifies the five main stages typical of the conduct of "any" PIA.
- It offers many questions to assessors and project managers that should be considered in carrying out a PIA.
- While a PIA is more than a compliance check, nevertheless the project manager must also comply with legislation, starting with Australia's Privacy Act.
- It encourages publication of the PIA report. If there are security, commercial-in-confidence or other competitive reasons for not making a PIA public in full or in part, the Commissioner encourages considering the release of a summary version.
- It contains templates (the modules) which can be used by assessors and/or project managers.
- Visitors to the website of the Office of the Privacy Commissioner can find a link for downloading the PIA Guide on the OPC's home page (other PIA guidance documents in other countries are harder to find).
- It includes a list of references to other PIA guidance documents and actual PIA reports.

Among the best elements from the OVPC *PIA Guide* are the following:

- The *Accompanying Guide* sets out various risks as well as possible strategies for mitigating those risks.
- It also sets out risks relating to other types of privacy in addition to informational privacy, i.e., bodily privacy, territorial privacy, locational privacy and communications privacy.
- The template provides the structure of a PIA report, which the user can adapt to his or her circumstances. The template has been produced as a Word document for ease of use by the assessor.
- The *Guide* draws on the experience of others to make the *Guide* more practical and effective.
- The *Guide* uses (p. 5) the word "project" to encompass any type of proposed undertaking, and explicitly includes "legislation" and "policy".
- It points out that a project need not be large, nor is the size or budget of a project a useful indicator of its likely impact on privacy. The project does not even need to involve recorded "personal information" as defined under the Information Privacy Act; a program that may include the need for bodily searches can still impact on privacy even if no personal information is recorded.
- The *Guide* recommends that a simple threshold privacy assessment be routinely conducted for every project. It includes a set of simple yes/no questions, an affirmative answer to any of which indicates that the organisation should seriously consider initiating a PIA.
- The *Guide* says up-front commitment from an organisation's executive to the conduct of PIAs is needed as the first step towards ensuring buy-in to the PIA's eventual recommendations.
- The *Guide* generally recommends publication of the report, but recognises some considerations, such as security, may influence the decision to publish. In such cases, it says that a properly edited PIA report will usually suffice to balance the security and transparency interests.

3 CANADA

3.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

In this chapter, we examine the privacy impact assessment framework in Canada at the federal level and in two provinces, Ontario and Alberta. In Annex 2, we provide some additional information about the legal basis of PIA in a third province, British Colombia.

3.1.1 Federal government

In Canada, policy responsibility for privacy impact assessment in the federal government lies with the Treasury Board of Canada Secretariat (TBS), which defines PIA as "a policy process for identifying, assessing and mitigating privacy risks".[1]

TBS promulgated a new Directive on Privacy Impact Assessment in April 2010.[2] The directive replaces the Privacy Impact Assessment Policy which had been in force since 2002[3] and data matching components of the 1993 Privacy and Data Protection Policy. The new directive applies to government institutions, but not to the development of new legislation.

The directive states that the Government of Canada is committed to ensuring that privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information.

Under the Privacy Act, a collection or grouping of personal information is referred to as a personal information bank (PIB). The President of the Treasury Board, as designated Minister, is responsible for registering all PIBs and reviewing the manner in which they are maintained and managed in all government institutions.

The directive further states that "government institutions routinely perform broad risk management activities and develop risk profiles related to their programs and activities. The PIA is the component of risk management that focuses on ensuring compliance with the Privacy Act requirements and assessing the privacy implications of new or substantially modified programs and activities involving personal information." This statement is important because it places PIA within risk management and because PIA is not only viewed as an activity to ensure compliance with the Privacy Act, but also for assessing privacy implications of new or modified programs and activities. Thus, the implication here is that it is not sufficient for government institutions to ensure compliance with the Privacy Act. They have to go beyond that to assess privacy implications not covered by the Privacy Act.

The directive goes on to say that if a PIA is "not properly framed within an institution's broader risk management framework, conducting a PIA can be a resource-intensive exercise. As such, the government is committed to ensuring that a PIA is conducted in a manner that is

[1] Treasury Board of Canada Secretariat, Policy on Privacy Protection, Ottawa, 1 Apr 2008. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text

[2] Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 Apr 2010. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text

[3] Treasury Board of Canada Secretariat, "Privacy Impact Assessment Policy", Ottawa, 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text

commensurate with the privacy risk identified and respects the operating environment of the government institution." It is not clear what the last bit – "respects the operating environment" means in practice. It is also not clear who identifies the privacy risk, nor how the risk is identified. It would be useful to engage stakeholders in the process of identifying the privacy risks as well as options or solutions for avoiding or mitigating those risks, but the directive makes no provision for engaging stakeholders.

The directive says heads of government institutions are responsible for establishing a PIA development and approval process and for ensuring that the PIA is completed by the senior official or executive with responsibility for new or substantially modified programs or activities.

The directive ties PIAs with submissions to the Treasury Board for program approval and funding. This is one of the strongest features of Canadian PIA policy. This linkage is spelled out in section 6.2 and Appendix B of the directive. Section 6.2 says that heads of government institutions are responsible for "adhering to the specific obligations related to PIAs and the Treasury Board submission process". Appendix B further specifies that government institutions seeking Treasury Board approval for programs or activities must:

- Initiate a PIA at the earliest possible phase of project planning;
- Identify whether a PIA has been completed in the body of the submission and, if a PIA was not completed because of the urgency or priority of the initiative, identify when the PIA is to be completed;
- Identify the measures taken or to be taken to address privacy issues and risks; and
- Complete a PIA before implementation of the new or substantially modified program or activity or within such time and subject to such conditions established by TBS.

The directive spells out that government institutions are to initiate a PIA:

- when personal information is used for or is intended to be used as part of a decision-making process that directly affects the individual;
- upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose; and
- when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities.

In instances of PIAs involving two or more government institutions, the directive favours one institution taking the lead and envisages a co-ordinating interdepartmental committee comprising key (governmental) stakeholders. It favours a single, overarching or multi-institutional PIA, rather than separate PIAs undertaken by individual departments.

In any case, the directive specifies that PIAs have to be signed off by senior officials, which is good for ensuring accountability, before a submission is made to the Treasury Board. The PIA is to be "simultaneously" provided to the Office of the Privacy Commissioner "along with any additional documentation that may be requested by that office".[4] Furthermore, institutions are instructed to make parts of the PIA publicly available, i.e., an overview and PIA "initiation",

[4] The directive points out that the Privacy Commissioner, as an officer of Parliament (as distinct from the government administration), has "broad powers of investigation… and can request additional project documentation related to the planning, assessment or implementation of new or substantially modified programs or activities that involve personal information or have an impact on the privacy of Canadians and of those individuals present in Canada". See section 8.2.1 of the directive.

and specified "risk area identification and categorisation" (a to h), which are listed in Section II of Appendix C of the directive (see below). Exceptions to public release are permitted for security as well as "any other confidentiality or legal consideration".

The TBS has laid down certain monitoring and reporting requirements in its Policy on Privacy Protection which also apply to the PIA directive – i.e., heads of government institutions are responsible for monitoring and reporting their compliance with the PIA directive and the TBS "will monitor compliance with all aspects of this policy by analyzing and reviewing public reporting documents required by the Privacy Act and other information, such as Treasury Board submissions", among other things.[5]

The TBS does not approve PIAs; it only reviews them to ensure that "the assessment is complete" (section 8.1.1 of the directive). It does say, however, that it will review the "core PIA" (in Appendix C of the directive) annually and, if necessary, propose amendments. The core PIA "consists of those standardized elements of a PIA that are directly linked to policy and legal compliance". This could be construed as suggesting a PIA is an exercise in compliance only, but this might be an unfair interpretation as the directive, as mentioned above, views privacy impact assessment as part of risk management, and risks may arise even if a project complies with legislation.

Appendix C of the directive sets out the minimum content of a core PIA, which must identify the government institution initiating the PIA, the head of the government institution, the senior official responsible, the name and description of the program or activity of the government institution, its legal authority for the program or activity, whether the proposal relates to a new or substantially modified PIB, a short description of the project and, in the instance of a multi-institutional PIA, the lead department.

The core PIA must also include a risk identification and categorisation, which uses a numbered scale, from 1 representing the lowest level of potential risk to 4, the highest level. The greater the number of risk areas identified as level 3 or 4, the more likely it is that the risk areas will need to be addressed more comprehensively. The risk areas relate to the type of program or activity, the type of personal information involved and context, the partners and private sector involvement, duration of the program, the program population, technology and privacy, personal information transmission and the risk of a privacy breach.

The PIA must also include additional elements, but these do not need to be made public. These other elements include:

- An analysis of personal information elements for the program or activity
- The flow of personal information
- A privacy compliance analysis, which must cover collection, retention, accuracy, disclosure, safeguards, technology and privacy issues
- A summary of analysis and recommendations
- A list of supplementary documents
- Formal approval, whereby the institution must indicate that the PIA has been formally approved.

While these are stated as the minimum elements of a core PIA, they convey to the reader that the emphasis on the PIA is completion of a PIA report, rather than emphasising PIA as a

[5] TBS, Policy on Privacy Protection, 2008, section 6.3.3.

process. The directive makes no provision for stakeholder engagement. Nor does it address the benefits of undertaking a PIA and finding solutions to privacy risks[6].

The PIA Guidelines

While the directive does not refer to the TBS's PIA Guidelines[7], these are still recommended even if they have not been revised since August 2002. The Guidelines are 40 pages long and divided into six chapters consisting of an Introduction, Purpose, Proceeding with a PIA, Process Overview, Detailed Process Description, Privacy Impact Analysis Report. There are three annexes providing a Table of Contents of a PIA, Table of Contents of a Preliminary PIA and an Example of a Summary Table. Key points from the Guidelines are extracted in the following paragraphs.

When to do a PIA

The first step in the PIA process is to determine whether it is required, and the first question to ask is, "Is personal information being collected, used or disclosed in this initiative?" If the answer is "no", then a PIA is not warranted. If the answer is "yes" or "maybe", officials should then go through the checklist of 11 questions on the first page of the guidelines. Among the questions are these:

2. Does the program require you to collect, use or disclose any personal information, such as name, address, age, identifying number, educational, medical or employment history, etc.?
6. Will the personal information generated by the program be used in decision-making processes that directly affect individuals, such as eligibility for programs or services or in enforcement activities?
8. Will the personal information be shared with any other organizations for any purposes other than for which it was originally collected?
9. Are you introducing new common client identifiers or are using the SIN [social insurance number] without any legislative authority?
10. Do you anticipate that the public will have any privacy concerns regarding the proposed program or service?
11. Are you introducing changes to the business systems or infrastructure architecture that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information?

These questions are somewhat like those in the privacy threshold assessment used in the Australian and Victoria PIA Guides, among others. Also like those guides, the TBS PIA Guidelines are based upon privacy principles, in this case those in the Canadian Standards Association's *Model Code for the Protection of Personal Information*[8] as well as federal privacy legislation and policies.

[6] Although the PIA Directive does not mention benefits or solutions, the PIA Guidelines do mention potential outcomes, which can be regarded as benefits or solutions.

[7] Treasury Board of Canada Secretariat, Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks, Ottawa, 31 August 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp. In an e-mail dated 8 July 2011 to the editor of this PIAF deliverable, a TBS spokesperson said that although Guidelines "predate the current Directive on Privacy Impact Assessment, much of the analytical guidance contained therein is still sound…. The new Directive has greatly lightened the administrative burden surrounding the reporting of PIAs and eliminated the need for Preliminary PIAs…. We are in the process of developing guidance around the new Directive which will be made available on the IPPD website at http://www.tbs-sct.gc.ca/ip-pi/index-eng.asp in the coming months."

[8] http://www.csa.ca/cm/ca/en/privacy-code

The Guidelines describe (p. 2) PIA as a "cooperative process" similar to "continuous" risk management. Elsewhere (p. 6), PIA is described as a continuous process that requires updating to reflect program, service or system changes". The process includes planning, analysis and education activities and "brings together a variety of skill sets to identify and assess privacy implications". These skill sets would seem to come from internal stakeholders. Elsewhere (p. 7), the Guidelines mention skill sets including privacy expertise, legal expertise, operational program and business design skills, technology and systems expertise, and information and records-keeping skills. Departments and agencies may also choose to involve their internal auditors. The Guidelines make little mention of consultation with external stakeholders as an intrinsic part of the PIA process (unlike the UK ICO Handbook, for example).[9]

Goals of a privacy impact assessment

Other PIA guidance documents state that the purpose of a PIA is to identify and mitigate privacy risks. Interestingly, the TBS Guidelines state that "a key goal of the PIA is to effectively *communicate* the privacy risks… [and] to contribute to senior management's ability to make fully informed policy, system design and procurement decisions". They also identify a set of specific goals most of which are communicative in orientation. These are:

- Building trust and confidence with citizens;
- Promoting awareness and an understanding of privacy issues;
- Ensuring that privacy protection is a key consideration in the initial framing of a project's objectives and activities;
- Identifying a clear accountability for privacy issues so that it is incorporated into the role of projects managers and sponsors;
- Reducing the risks of having to terminate or substantially review a program or service after its implementation in order to comply with privacy requirements;
- Providing decision-makers with the information necessary to make informed policy, system design or procurement decisions based on an understanding of the privacy risks and the options available for mitigating those risks; and
- Providing basic documentation on the business processes and flow of personal information for common use and review by the department's staff and as the basis for consultations with stakeholders, specifications, information privacy procedures and communications.

These are, of course, all laudable goals. It is instructive to note that accountability is one of the principal goals and the reference to consultations with stakeholders.

Privacy risks

The Guidelines identify several common privacy risks:

- *Data profiling/data matching*: combining unrelated personal information obtained from a variety of sources to create new information about an individual or using information about an individual's preferences and habits to build a profile on the individual.

[9] The first questionnaire in Chapter 5 of the PIA Guidelines contains two questions about consultation: "Where appropriate, have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposal? Where appropriate, will public consultation take place on the privacy implications of the proposal?" The second questionnaire, for cross-jurisdictional programs and services, has two identical questions.

- *Transaction monitoring*: observing or tracking the history of an individual's interaction with one or more programs or services. This usually results in creation of new personal information describing an individual's overall experience with one or more programs.
- *Identification of individuals*: electronic service delivery generally requires identification of an individual and authentication of their identity as way of managing security risks. Surveillance risks exist where the use of common identifiers or identification systems facilitate data sharing, profiling or transaction monitoring.
- *Physical observation of individuals*: tracking the movement or location of an individual through the use of vehicle transponders, satellite locators, cameras or mechanisms for recording an individual's use of kiosks.
- *Publishing or re-distribution of public databases containing personal information*: electronic publishing frequently eliminates practical limits on the misuse of information, as it can be easily manipulated and used for purposes entirely unrelated or is intended use in manual form.
- *Lack or doubtful legal authority*: failure to identify clear program authority to collect, use or disclose personal information raises concerns about whether an initiative should be undertaken on both the privacy front and with respect to the Charter of Rights and Freedoms Act.

Process overview

The Guidelines say the PIA process has four main steps, which are broadly similar to those mentioned above in Australia. The four steps are project initiation, data flow analysis, privacy analysis and preparation of a privacy impact analysis report.

Step 1: Project initiation

One of the first steps is to **determine the scope** of the PIA and the resource requirements, including the knowledge and skills needed to develop and maintain the PIA. "The nature and extent of resources required for a PIA will vary depending on the scope and complexity of the proposal." The Guidelines distinguish between a "preliminary PIA" and a "full PIA"; however, as noted in the footnote above, the TBS intends to do away with the notion of a preliminary PIA. They also state (p. 4) that PIA is "a dynamic process and as design changes occur in the business processes, the PIA should also be reviewed and updated". The Guidelines recognise implicitly that there is no such thing as a one-size-fits-all PIA. "Departments and agencies are encouraged to adapt it to fit their particular needs." The Guidelines say departments and agencies should consider undertaking generic or overarching PIAs where proposals are similar or interrelated because individual PIAs would be a duplication of effort.[10] In the interests of accountability, the deputy head of the government institution is responsible for compliance with privacy requirements, but he could choose a senior executive, such as the privacy co-ordinator, to be in charge of the PIA. The Guidelines say only one individual should be assigned responsibility for the co-ordination and completion of the PIA.

Step 2: Data flow analysis

This activity involves a description and analysis of the business context, the information flows and the systems and infrastructure contemplated for the proposal. The Guidelines encourage (p. 7) creation of a "business flow diagram" showing how personal information is collected,

[10] The European RFID PIA Framework adopts a similar approach.

used, disclosed and retained as well as documenting the physical or logical separation of personal information or security mechanisms that prevent improper access to personal information.

The Guidelines suggest construction of a "data flow table", like the following:

Description of personal information cluster	Collected by	Type of format (e.g. paper, electronic)	Used by	Purpose of collection	Disclosed to	Storage or retention site

The Guidelines regard the business flow diagram as "a critical communications vehicle", which should be readily understood by officials from various backgrounds.

Step 3: Privacy analysis

The privacy analysis examines the data flows in the context of applicable privacy policies and legislation. The Guidelines include two questionnaires to help identify privacy risks or vulnerabilities in the proposal and to facilitate the privacy analysis. The questionnaires include a yes or no field as well as a "Provide details" field for explaining how a particular requirement is met or why it is not met.

The Guidelines say that officials should complete one or the other questionnaire. The first set of questions is derived from the requirements of the Privacy Act and "dovetail" with the universal privacy principles. The second questionnaire is intended for cross-jurisdictional programs or services, and each jurisdiction should complete its own PIA based on its specific statutory and policy provisions.

The results from completing the questionnaire are used to form the PIA Report.

Step 4: Privacy impact analysis report

This step involves a documented evaluation of the privacy risks and the associated implications of those risks along with a discussion of possible remedies or mitigation strategies. The PIA report should be "designed as an effective communications tool used by a variety of stakeholders".

The Guidelines say that departments and agencies can undertake generic or overarching PIAs where proposals are similar or interrelated to avoid duplication of effort.

Chapter 5 of the Guidelines provides a more detailed description of the PIA process, of the four steps mentioned above, and sets out the two above-mentioned questionnaires.

The first questionnaire has questions relating to

- the accountability of personal information
- the collection of personal information
- consent
- use of personal information
- disclosure and disposition of personal information

- accuracy of personal information
- safeguarding of personal information
- openness
- individual's access to personal information
- challenging compliance.

The second questionnaire, prepared for cross-jurisdictional programs and services, is structured in the same way as the first. The questions are based on 10 principles reflecting those in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information. The questions concern

- accountability
- identifying purposes
- consent
- limiting collection
- limiting use, disclosure and retention
- accuracy
- safeguards
- openness
- individual access
- challenging compliance

Chapter 6 of the Guidelines concerns the privacy impact analysis report. As part of the analysis, departmental representatives are exhorted (p. 34) to develop possible solutions for each privacy risk and an accompanying action plan to be used by the department or agency to ensure that privacy is managed effectively throughout the process.

The PIA report should convey the following information:

1. A detailed description of the proposal including objectives, rationale, clients, approach, programs and/or partners involved. Departments should take into consideration the environmental context in which the proposal is being made and the public's expectations regarding privacy.
2. A list of all the data elements that involve "personal information" and a related description.
3. A list of all stakeholders and their roles and responsibilities.
4. A list of relevant legislation and policies that have a bearing on privacy requirements of the proposal.
5. A description of the specific privacy risks that have been identified and an indication of the level (low, medium or high) of risk involved. Departments can choose to complete a summary table to display the risks and their implications for a proposal. Use of the table is optional since some privacy experts recognise that it is difficult to assess both the likelihood and impact of risks.
6. Options to eliminate or mitigate privacy risks, with a statement of the implications associated with those mechanisms where relevant.
7. A description of any residual or outstanding risks that cannot be addressed through the mitigation mechanisms. Where appropriate, departments should include references to and a description of public opinion or expectations regarding those residual risks.
8. An outline of a privacy-oriented communications strategy, if the implementation of such a strategy is considered appropriate.

Departments and agencies are reminded to provide a copy of the final PIA report to the Privacy Commissioner and prepare an executive summary for public consumption. Interestingly, the Guidelines say (p. 35) that "The Office of the Privacy Commissioner has requested that departments and agencies do not publish any of their [the OPC's] comments." One would have thought that knowing the OPC's comments would help stakeholders, including the public, to assess the privacy impacts of any new project.

Benefits (outcomes)

The Guidelines say (p. 36) potential outcomes (= benefits) of a PIA include the following:

- Use of anonymous information in place of personal information to achieve the same program objectives;
- Cost avoidance by considering privacy at the outset thus avoiding exponential design costs associated with retrofitting requirements at a later development stage;
- Building of public trust and confidence that privacy has been built into the design of the program or service;
- Where risk cannot be mitigated through technical or policy instruments, a PIA will provide decision-makers with a full assessment of the risk;
- A possible decision to abandon a project at an early stage based on the significance of the privacy risks;
- A disciplined process that promotes open communications, common understanding and transparency.

The Guidelines conclude with annexes illustrating a sample table of contents for a PIA report and an example of a summary table.

3.1.2 Ontario

In Ontario, since the late 1990s, the principal driver behind government policy in relation to PIAs was not the privacy oversight body, but a central agency called the Management Board Secretariat (MBS). As early as June 1998, a completed PIA became a pre-requisite for approval of Information and Information Technology (I&IT) project plans submitted for Cabinet approval.[11]

The mandate to complete PIAs in the Ontario public service derives primarily from the Information & Information Technology Directive and the Procurement Directive, both issued under delegated authority of the Management Board of Cabinet. The requirement is also contained in the Corporate Policy on Protection of Personal Information and the information technology project review processes. In December 2010, Ontario's central agency, the Office of the Information and Privacy Commissioner released a revised PIA guide, replacing the 2001 version. The guide provides an overview of the PIA methodology and outlines the privacy activities required throughout a project's lifecycle. It also explains how to integrate a PIA into project management and use the results to meet the corporate governance requirements. Three PIA tools were also released at that time and provide detailed

[11] Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", *Computer Law & Security Review*, Vol. 25, No.2, April 2009, pp. 123-135 [p. 127]. PrePrint at http://www.rogerclarke.com/DV/PIAHist-08.html

instructions, checklists, templates and other resources to help projects complete the PIA process. It is too early to draw conclusions on their use. [12]

Section 6 of the Regulation to the Personal Health Information Protection Act (PHIPA) mandates PIAs for Health Information Network Providers (HINP), when two or more Heath Information Custodians (HIC) use electronic means to disclose Personal Health Information (PHI) to one another. In this respect, the legislative and policy drivers for this come from the government. Furthermore, 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.[13]

The *Privacy Impact Assessment Guide* for the Ontario Public Service (hereafter PIA Guide)[14] is a 69-page document and is accompanied by three other documents, Preliminary Analysis (Part 1, 39 pages), Privacy Risk Analysis (Part 2, 36 pages) and Privacy Design Analysis (Part 3, 95 pages). Although these documents are marked "Unclassified", none of them is available on the Ontario government's public website, although they are available on the government's intranet and can be obtained by requesting them.[15] They are not posted on the government's public website nominally because they are aimed at government departments and for financial reasons (squeezing out a budget for translation of the documents into French seems problematic).[16]

The Guide is divided into five sections – an Introduction, Context, PIA Overview, Integrating Privacy into Project Management and Corporate Governance Processes, and Appendices.

Ultimate accountability for privacy protection rests with the Minister, as head of each government institution. The head is responsible for complying with Freedom of Information and Protection of Privacy Act (FIPPA) and for ensuring that personal information held by the ministry is accurate, up to date and collected, used and disclosed only as authorised.[17]

The Guide defines privacy impact assessment as "a consistent and systematic approach for identifying and analysing privacy risks when changing or developing programs or systems".[18] It is also described as "both a due diligence exercise and a risk management tool".

Antedating this Guide, the Office of the Information and Privacy Commissioner/Ontario (IPC) prepared a *Privacy Impact Assessment Guidelines for Ontario's Personal Health Information Protection Act*.

[12] Bayley, Robin, and Colin J. Bennett, "Privacy impact assessments in Canada", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
[13] Tancock, David, Siani Pearson and Andrew Charlesworth, "Analysis of Privacy Impact Assessments within Major Jurisdictions", in *Proceedings of the 2010 Eighth Annual International Conference on Privacy, Security and Trust*, Ottawa, 17-19 Aug 2010, published 30 Sept 2010, pp. 118-125 [p. 121].
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5593260
[14] Office of the Chief Information and Privacy Officer (OCIPO), Privacy Impact Assessment Guide for the Ontario Public Service, Queen's Printer for Ontario, December 2010.
[15] Contact the Information, Privacy, and Archives Division (IPA) at iNetwork@ontario.ca.
[16] E-mail dated XX July 2011 to the editor from an official of the Office of the Chief Information and Privacy Officer.
[17] Ontario PIA Guide, p. 4.
[18] Ibid., p. 5.

Like other PIA guidance documents, the 2010 PIA Guide says a PIA should be started as early in a project's lifecycle as possible. For a program already in place, officials wishing to assess the adequacy of privacy protections can refer to the *Guide and Checklist for Managing Personal Information.*

Various government directives require a PIA. The Information & Information Technology (I&IT) Directive requires ministries and agencies to complete a PIA whenever there is a substantive change in the collection, use or disclosure of personal information. The Procurement Directive requires ministries to do a PIA prior "to undertaking any procurement of goods and/or services that may result in the release of personal or sensitive information".

It seems preparation of the Ontario PIA Guide has taken into account other PIA guidance documents. It specifically refers to the PIA Guide prepared by the Office of the Victoria Privacy Commissioner as well as that of the Australian Office of the Privacy Commissioner.

The Ontario PIA Guide says there are three separate, but related parts to a PIA:

1. Preliminary analysis – All projects required to complete a PIA must complete a preliminary analysis, to determine whether the project will involve personal information and needs to be protected in accordance with FIPPA. The Preliminary Analysis (Part 1) document contains a set of questions, the responses to which are to be submitted to the IPA, whose review is to help verify conclusions and identify the assessor's next steps.[19]
2. Privacy risk analysis – looks beyond just compliance with FIPPA, to identify a project's privacy risks (legal, policy, technology and enterprise), their likelihood, impact and priority for action, and what needs to be done to address them, optimally before the direction of a project is set. "In essence, it will tell you if your project should 'stop', 'go' or 'proceed with caution'."
3. Privacy design analysis – is used identify how to make a project comply with FIPPA. While the privacy risk analysis looks at the broad privacy implications of your project, the privacy design analysis focuses on specific legislative requirements. Privacy must be designed into systems as an integral part of the technology design process. It involves a step-by-step review (identification) of your business processes; roles and responsibilities; systems, applications and related technology; data flows of personal information (i.e., how it will be collected, used, retained, disclosed and destroyed, by whom and for what purposes); privacy risks, their likelihood, impact and priority for action, and what needs to be done to address them as well as a thorough analysis of the requirements related to the protection of personal information and recommendations to make the project comply with privacy rules. The Guide says the privacy design requirements are the "road map" for how a project will need to proceed.

Privacy is one of the key risks projects must address as it can significantly impact policy, business, I&IT and procurement decisions. Like other PIA methodologies, the Guide views PIA as part of risk management, project management and IT governance. The PIA needs to inform, and be informed by, a threat risk assessment (TRA).

Scope and scale of the PIA

Like other PIA guidance documents, the Ontario PIA Guide makes the point (p. 13) that there is no one-size-fits-all PIA. It goes on to say that every project is different. The PIA activities in the Guide are designed to accommodate large or enterprise-wide projects (i.e., those that

[19] Preliminary Analysis (Part 1), p. 5.

impact a large number of people or involve a large quantity of personal information or involve numerous program areas), but they can be adapted for initiatives of any size or complexity. It says the privacy analysis needed for a small project is the same as for a large project; however, the level of detail of the PIA should be consistent with the requirements of the project. The scope and scale of the project will determine the scope and scale of the PIA.

PIA documentation

One of the key deliverables of the PIA is documented assurance that privacy risks related to a project, including residual risks, have been identified and addressed. The Guide says it is important to document activity, analysis, findings and recommendations throughout the PIA for several reasons:

- the project sponsor (i.e., the accountable decision-maker) is required to sign off project documents informed by the PIA findings;
- to demonstrate privacy "due diligence";
- program areas may need to revisit privacy issues once the project has concluded — sometimes years later;
- related or similar initiatives may need to understand how decisions impacting privacy were made and their rationale; and
- if there is a privacy breach or other incident resulting from an unaddressed privacy risk, justification for accepting that risk may be needed.

Deliverables (= PIA report)

The Guide suggests that the PIA deliverable identify:

- resolved privacy risks to date, and how they were addressed;
- outstanding privacy risks, assessment of likelihood, harm and priority for action;
- recommended course of action for outstanding privacy risks;
- residual privacy risks and implications.

As the project is implemented, the Guide recommends that the appropriate person in charge of the PIA:

- monitor progress of privacy-related activities to make sure they are appropriately completed (i.e., in accordance with approved privacy design requirements);
- identify and assess new, outstanding and residual privacy risks; and
- alert the project sponsor (= the project manager) to any privacy-related problems that need to be addressed.

The PIA Guide makes no mention of consulting stakeholders or a third-party audit of the PIA or publication of the PIA report. The Guide mostly focuses on personal information, rather than all types of privacy – but see the paragraph following the next.

There is some good, quotable text in the PIA Guide, which otherwise is rather bureaucratic in its literary style. One of those texts is this: "Privacy protection is not a barrier to doing the business of government — it helps to define what that business is."[20]

[20] Ontario PIA Guide, p. 36. Another good quote in the Guide comes from the Supreme Court of Canada: It stated that "society has come to realize that privacy is at the heart of liberty in a modern state … Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual". R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.).

It says there are three main reasons why a project needs to protect privacy:

- First, to meet legislative obligations;
- Second, to preserve public trust – "Government has a legal and ethical responsibility to protect the data entrusted to it. A breach in privacy is a breach of trust."
- Third, to address broader privacy issues – the Guide says it is important to look at other types of privacy when assessing a project, i.e., freedom in their physical domain, freedom of movement or expression or of the person or personal space; freedom to communicate privately with others; freedom to determine when, what, how and with whom they share their personal information.

It adds that "An activity may comply with the law but still be seen as unnecessarily privacy invasive."[21]

Appendix E of the Guide concerns privacy risk management methodology. It says that risk management is an essential component of good management, that every manager is responsible for identifying and documenting all significant risks and that privacy is one of the key risks for any program area involving the public.

Three types of risk

Appendix E identifies three types of risk:

- a *privacy risk* is something that could jeopardise or negatively impact someone's privacy, such as any unauthorised collection, use or disclosure, as it creates the potential for harm, including identity theft and other forms of fraud, physical safety issues such as stalking or harassment, financial loss, adverse impact on employment or business opportunities, or damage to reputation.
- an *organisational risk* is something that could negatively impact a government institution, such as:
    - public outcry as a result of a perceived loss of privacy or failure to meet expectations regarding privacy protection;
    - damage to a ministry's public image and loss of public trust or confidence;
    - public embarrassment for a minister and senior executives due to an investigation by the Office of the Information and Privacy Commissioner (IPC), questions in the Legislative Assembly or negative media attention;
    - operational disruptions, inefficiencies and ineffectiveness that impact continuity and quality of service; and
    - contravention of contractual requirements.
- a *legal risk* is created because of non-compliance with FIPPA – this type of risk impacts both the data subject and the organisation.

It notes that any project involving the collection, use, retention, disclosure or destruction of personal information may create privacy risks if not properly designed and managed. It states that "The potential damage to the individual must take precedence in your assessment over organizational risks."[22] It also adds that "Risk management can mitigate a risk, but it can never be completely avoided or eliminated. If your project involves personal information, there always will be some privacy risk."

[21] Ontario Privacy Guide, p. 37.
[22] Ibid., p. 48.

Appendix F contains a set of questions relating to business processes and architecture, governance, collection, use, disclosure, accuracy, retention, disposal and destruction, safeguards, access and correction, complaints, openness and accountability. A "yes" answer indicates an area that needs to be examined, along with an explanation and a recommended course of action.

3.1.3 Alberta

In 2001, the Office of the Information and Privacy Commissioner (OIPC) of Alberta introduced its first Privacy Impact Assessment (PIA) questionnaire. In the following eight years, according to the OIPC, the practice of privacy impact assessments matured and the number of PIAs increased dramatically. In January 2009, the OIPC revised the PIA template and guidelines.[23]

Those submitting PIAs are told to consider the feedback from the OIPC before they implement their projects. Otherwise, if the OIPC identifies privacy concerns, "it may be necessary to make expensive and time-consuming changes to your project late in the development cycle".[24] The OIPC appears to exercise much more power than most of its counterparts. Not only are PIAs mandatory, they must be submitted to the OIPC before implementation of a new system or practice. If the OIPC finds shortcomings, projects can be turned down or forced to make costly retrofits. It appears to play a much more activist role in reviewing PIAs.

The OIPC says it will try to provide preliminary results of its review of a PIA within 45 days. The time from preliminary review to its acceptance of the PIA depends on how quickly the custodian (= project manager) resolves any questions raised by the OIPC. The OIPC points out that "acceptance" is not approval. It only reflects the OIPC's opinion that the project manager has considered the requirements of the HIA and has made a reasonable effort to protect privacy.

The OIPC says custodians should review their PIAs as new practices and technologies evolve after projects are implemented and new threats to privacy may also develop. Custodians should advise the OIPC of any resulting changes to the PIA. The OIPC says if a member of the public makes a complaint against the custodian's organisation, it may review previously submitted PIAs.[25]

Under section 64 of the HIA, custodians must submit a PIA whenever they plan to implement new administrative practices or information systems that collect, use or disclose health information about identifiable individuals. This also applies to changes to practices or systems. Under sections 70 and 71, custodians must also prepare a PIA before performing data matching, which is defined as the creation of new information by combining two or more sets of data.

Under section 8(3) of the Health Information Regulation, custodians must periodically review the adequacy of the safeguards they have in place to protect health information privacy.

---

[23] Office of the Information and Privacy Commissioner (OIPC) of Alberta, *Privacy Impact Assessment (PIA) Requirements For use with the Health Information Act*, January 2009. www.OIPC.ab.ca
[24] OIPC, 2009, p. 5.
[25] OIPC, 2009, p. 6.

Unlike other PIA methodologies that say PIAs should be initiated as early as possible, the OIPC PIA Requirements say that, generally speaking, the best stage to do a PIA is after all business requirements and major features of the project have been determined in principle, but before completing detailed design or development work to implement those requirements and features, when it is still possible to influence project design from a privacy perspective.[26]

The PIA must include details on the project's information security and privacy policies and procedures.

The Alberta PIA Requirements are unusual in making mandatory the format for HIA PIAs. Submissions must include the following sections:

- A cover letter signed by the custodian or authorised representative.
- A cover page, which provides basic information about the PIA and contact information for people involved in the PIA process.
- Section A, **project summary** describes the project to be assessed, its objectives, business rationale, key players, why it must collect, use or disclose personal health information and where the information is to be stored. The OIPC publishes summaries of all accepted PIAs in an **online PIA registry**. Section A information will be posted in the registry.
- Section B, **privacy management** describes the engagement of the organisation's senior management in setting privacy policy and resolving privacy issues. It specifies to whom the organisation's privacy officer and/or HIA co-ordinator reports and whether there is a privacy committee. It should describe how the organisation develops its privacy policies, who approves them, how they are communicated to employees, how often they are reviewed. It should describe how employees and contractors are trained in privacy and how often. It should describe how the organisation identifies, investigates and manages a privacy incident, which the OIPC defines as an event that adversely affects the confidentiality, integrity or availability of health information. It should describe how the organisation manages requests from individuals to access their own health information and to make corrections.
- Section C, **project privacy analysis** lists the health information that is collected, used or disclosed in the project. It should give defensible reasons for such collection, use or disclosure of each piece of information and how it contributes to the objectives of the project. It must list unique identifiers, i.e., data elements that uniquely identify a single individual, such as name, account number, etc. This section should provide an information flow analysis supported by a diagram and table that describes the purposes and legal authority for each collection, use and disclosure of health information. The information flow diagram illustrates how health information is collected, used and disclosed beyond the project or organisation. Each information flow can be numbered and cross-referenced in the table which documents each category of information collected, used or disclosed, for a clearly defined purpose and supported by specific sections of appropriate legislation. This section should describe how individuals will be notified of all purposes for which their health information is collected, why it is being collected and how it will be used and the specific legal authority that authorises the collection. It should provide contact details for someone in the project manager's organisation who can answer any questions about the collection. The PIA should describe the role played by individual consent in the project. It should state whether the health information from the project will be linked, matched or otherwise combined with information from other sources and, if so, how

[26] OIPC, 2009, p. 13.

the linkage will occur and its purpose. It should describe and provide copies (or relevant sections of) contracts or agreements with third parties involved in the project (such as for IT support). It should describe how and why information from the project is used in jurisdictions outside Alberta. The risks of such transfers need careful assessment and mitigation.

- Section D, **project privacy risks and mitigation plans** should be described in as much as detail as possible. The PIA should describe how persons, positions, employee categories or third parties are given access to specific health information data elements. It should state who has access to the information, the nature of the information, the circumstances under which they have access, the type of access, and the purpose or reason for the access. This section should identify specific privacy risks for the project, the circumstances that lead to the risks within the project and how these are to be mitigated using a combination of administrative, technical or physical measures. More than one measure will likely be needed to address each risk (e.g., a policy, combined with a training program and an audit). This section should also describe plans for monitoring compliance with the privacy protection measures, how the results will be reviewed to improve the privacy and security of health information and who will conduct the reviews and audits. The PIA should be updated as necessary with notifications to the OIPC. Periodic reviews of privacy protection measures are mandatory under the HIA.
- Section E, **policy and procedures attachments** provide a list of privacy and information security policies specific to the project. The custodian must summarise in a table all of the policy and procedure documents provided with the PIA. He or she must attach copies of policy documents demonstrating that he or she has addressed the topics listed in the appendices. [27]

The OIPC advises custodians that if they do not provide enough detail, the OIPC will ask for clarification, which will increase the overall PIA review time and delay the project.

3.2 LEGAL BASIS

3.2.1 Federal level

1. General framework for privacy and data protection

The Canadian Charter of Rights and Freedoms,[28] being a part of the Canadian Constitution, is a basic fundamental rights protection instrument. It does not contain a right to privacy, yet courts have interpreted a right to a reasonable expectation of privacy from the prohibition from unreasonable search and seizure (Sec. 8 of the Constitution).

The general privacy and data protection in Canada on the federal level is the **Privacy Act** (1983),[29] regulating public sector. Provinces and territories have their own privacy laws for their pubic sector. The **Personal Information Protection and Electronic Documents Act (PIPEDA)**[30] (2000) applies to private sector commercial activities throughout the country,

[27] OIPC, 2009, pp. 16-33.
[28] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (United Kingdom), 1982, c. 11, s. 8. http://laws-lois.justice.gc.ca/eng/charter
[29] Privacy Act, R.S.C., 1985, c. P-21, http://laws-lois.justice.gc.ca/PDF/P-21.pdf.
[30] Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

with the exception of three provinces (Alberta,[31] British Columbia[32] and Quebec)[33] that have enacted "substantially similar" provincial legislation of their own. In addition, the Governor General in Council, pursuant to Sec. 77(1) of the Privacy Act, made a **Privacy Regulation** (1983).[34] Four provinces have passed legislation for the protection of information in the health sector: Ontario (Personal Health Information Protection Act, 2004), Manitoba (Personal Health Information Act), Saskatchewan (Health Information Protection Act) and Alberta (Health Information Act).[35]

Oversight of both federal Acts is handled by the Privacy Commissioner of Canada.[36] Provinces have their own information commissioners, e.g. Information and Privacy Commissioner of Alberta (OIPC).[37]

2. Laws on PIA forerunners

Nothing has been found.

3. PIA legal bases

In Canada, PIA has its legal basis in instruments issued on the level of a ministry. The three directives discussed below were issued pursuant to Sec. 71(1) of the Privacy Act that states:

> Subject to subsection (2), the designated Minister shall
> …
> (d) cause to be prepared and distributed to government institutions directives and guidelines concerning the operation of this Act and the regulations.

The President of the Treasury Board has been designated to act as a Minister for the purposes of the said Act, pursuant to Sec. 3(1)(1) of the Privacy Act.[38] All these instruments apply to government institutions, including parent Crown corporations and any wholly owned subsidiary of these corporations, but except the Bank of Canada.

The **Directive on Privacy Impact Assessment**,[39] effective from 1 April 2010, is a comprehensive legal basis for PIA in Canada. It replaced Privacy Impact Assessment Policy dated 2 May 2002. The current Directive states that

> 6.3 The appropriate senior officials or executives are responsible for adhering to the following process for the completion of a privacy impact assessment:

---

http://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest.

[31] Personal Information Protection Act, SA 2003, c P-6.5. http://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest.

[32] Personal Information Protection Act, BC Reg 473/2003. http://www.canlii.org/en/bc/laws/regu/bc-reg-473-2003/latest.

[33] An Act respecting the Protection of personal information in the private sector, RSQ, c P-39.1. http://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest

[34] Privacy Regulations, SOR/83-508, http://lois-laws.justice.gc.ca/PDF/SOR-83-508.pdf

[35] Privacy International, Privacy and Human Rights 2006. *Country Reports – Canada*. https://www.privacyinternational.org/article/phr2006-canada

[36] Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca

[37] Office of the Information and Privacy Commissioner of Alberta. http://www.oipc.ab.ca

[38] Designating the Minister of Justice and the President of the Treasury Board as Ministers for Purposes of Certain Sections of the Act, SI/83-109, Canada Gazette Part II, Vol. 1/7, No. 1, 22 June 1983. http://www.collectionscanada.gc.ca/obj/001060/f2/1980/cgc_p2-0_v117_n012_t000_000_19830622_p00208.pdf

[39] Directive on Privacy Impact Assessment. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoo=X&id=18308

A) Initiation of a privacy impact assessment

6.3.1 Initiating a PIA for a program or activity in the following circumstances:

- when personal information is used for or is intended to be used as part of a decision-making process that directly affects the individual;
- upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose; and
- when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities.

C) Completion of the privacy impact assessment

6.3.9 Completing the core PIA elements as outlined in Appendix C.

6.3.10 Determining an appropriate format for the PIA based on the government institution's business needs, internal reporting and broader risk management activities.

E) Notification and registration

6.3.14 Ensuring that the approved core PIA is provided to Treasury Board Secretariat (TBS) along with the proposed new or substantially modified PIB description, unless otherwise specified in the terms and conditions of a delegation under subsection 71(6) of the Privacy Act. TBS will only confirm that mandatory requirements of the core PIA have been completed for the purpose of establishing or revising a PIB. Because no additional documentation will be reviewed, none is to be provided to TBS for the purpose of reviewing and approving PIBs.

Appendix B – Privacy Impact Assessment requirements related to the preparation of Treasury Board submissions

Government institutions seeking Treasury Board approval for programs or activities that involve personal information are responsible for:

- Making every reasonable effort to initiate the PIA at the earliest possible phase of project planning;
- Identifying whether a PIA has been completed in the body of the submission and, if a PIA was not completed because of the urgency or priority of the initiative, identifying the timelines for the completion of the PIA;
- Identifying in their project brief the measures taken or to be taken to address privacy issues and risks, where relevant, when seeking project approval from Treasury Board;
- Completing a PIA for the new or substantially modified program or activity that was approved by Treasury Board either before its implementation or within such time and subject to such conditions established by TBS.

This Directive is to be read in conjunction with the Privacy Act, the Privacy Regulations, the Policy on Privacy Protection, Directive on Privacy Practices and Directive on Privacy Requests and Correction of Personal Information and the Directive on Social Insurance Number (*cf.* para 3.5).

The **Policy on Privacy Protection**,[40] effective from 1 April 2008, requires PIA be conducted:

6.2 Heads of government institutions or their delegates are responsible for:

…

6.2.14 Ensuring that, when applicable, privacy impact assessments (PIAs) and multi-institutional PIAs are developed, maintained and published.

[40] Policy on Privacy Protection. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

The **Directive on Privacy Practices**,[41] effective from 1 April 2010, also requires PIA be conducted:

> 6.1 Heads of government institutions or their delegates are responsible for the following:
> …
> 6.1.4 Ensuring that the development process for new or substantially modified PIBs [Personal Information Banks] is aligned with the process for the development and approval of the core privacy impact assessment (PIA).

The **Directive on Social Insurance Number**,[42] effective from 1 April 2008, requires PIA be conducted. Its Appendix B regulates obtaining policy approval:

> *Step 2 – Analysis and consultation*
> Before seeking approval from Treasury Board Ministers, the following process is required:
> - Submit a completed Privacy Impact Assessment (PIA) report related to the new collection or new consistent use to Treasury Board Secretariat's Information and Privacy Policy Division for review; and
> - Notify the Privacy Commissioner in compliance with section 6.2.12 of the Policy on Privacy Protection and subsection 9(4) of the Privacy Act.

All Directives mentioned in this section contain a provision on **non-compliance**. Each refers to section 7 of the Policy on Privacy Protection:

> 7. Consequences
> 7.1 For those government institutions that do not comply with this policy, its directives and standards, TBS will require them to provide additional information relating to the development and implementation of compliance strategies in their annual report to Parliament. This reporting will be in addition to other reporting requirements and will relate specifically to the compliance issues in question.
> 7.2 For those government institutions subject to the MAF [Management Accountability Framework], non-compliance, compliance and exemplary performance with respect to this policy, and related directives and standards will be reported in the assessment prepared as part of the MAF process.
> 7.3 On the basis of analysis of monitoring and information received, the designated minister may make recommendations to the head of the government institution. This could include prescribing any additional reporting requirements, as outlined in subsection 7.1 above.

4. Guidance material

In 2002, under the old PIA Policy, the Treasury Board of Canada Secretariat issued "*Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks*". In 2011, the Office of the Privacy Commissioner of Canada issued a guide for submitting PIA.[43]

In private sector, in April 2007 the Advanced Card Technology Association of Canada issued a design tool and a PIA template titled "*Contactless Smart Card Applications: Design Tool and Privacy Impact Assessment*".[44]

---

[41] Directive on Privacy Practices. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309
[42] Directive on Social Insurance Number. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342
[43] Office of the Privacy Commissioner of Canada, *A Guide for Submitting Privacy impact Assessments to the office of the Privacy Commissioner of Canada: Expectations*, 2011.
http://www.priv.gc.ca/information/pub/gd_exp_201103_e.pdf.

5. Proposals

In June 2006, the Office of the Privacy Commissioner of Canada on its website discussed a possible reform of the Privacy Act.[45] It calls for PIA introduction:

> The reporting requirements under section 72 of the Privacy Act should be strengthened in the interests of transparency. … These requirements would include, but not be limited to, the obligation to carry out Privacy Impact Assessments (PIAs) for new or substantially modified programs or policies (including new legislation), as well as the obligation to report on PIAs in the Annual Reports under s. 72 and, when and where appropriate, through the Departmental Performance Reports and other management representations to central agencies and Parliament.

On 29 April 2008, on appearance before the Standing Committee on Access to Information, Privacy and Ethics on Privacy Act Reform, the Privacy Commissioner recommended:[46]

> Enshrine a requirement for heads of government institutions subject to the Privacy Act to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

The Commissioner explained her rationale:

> There is no specific section requiring Privacy Impact Assessments as part of a sound privacy regime that should be in place for ensuring compliance with the Privacy Act and fair information principles. … In May 2002, the Treasury Board Secretariat … introduced an administrative policy on Privacy Impact Assessments.
> Given the unevenness with which government institutions are implementing the Privacy Impact Assessment policy, there should be a legal requirement for Privacy Impact Assessments to ensure that they are done on a consistent and timely basis. … In the OPC's 2007 audit of government compliance with the Privacy Impact Assessment policy, it was ascertained that institutions are not fully meeting their commitments under the policy. Privacy Impact Assessments are not always conducted when they should be. … Privacy Impact Assessments should be submitted to the OPC for review prior to program implementation.

The same recommendation on a similar appearance was made on 11 May 2009.[47]

3.2.2 Ontario

1. PIA legal bases

[44] Advanced Card Technology Association of Canada, *Contactless Smart Card Applications: Design Tool and Privacy Impact Assessment*, 2007. http://www.ipc.on.ca/images/Resources/act-pia.pdf
[45] Office of the Privacy Commissioner of Canada, *Reforming the Privacy Act*, June 2006. http://www.priv.gc.ca/information/pub/pa_reform_060605_e.cfm.
[46] Privacy Commissioner of Canada, *Appearance before the Standing Committee on Access to Information, Privacy and Ethics on Privacy Act Reform*, 29 April 2008. http://www.priv.gc.ca/parl/2008/parl_080429_02_e.cfm.
[47] Privacy Commissioner of Canada, *Appearance before the Standing Committee on Access to Information, Privacy and Ethics on Privacy Act Reform*, 11 May 2009. http://www.priv.gc.ca/parl/2009/parl_090511_02_e.cfm

Sec. 6 of the Ontario Regulation 329/04[48] to the **Personal Health Information Protection Act, 2004 (PHIPA)**[49] provides for PIA be conducted by "health information network providers" (HINP):

> (2) In subsection (3), "health information network provider" or "provider" means a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.
>
> (3) The following are prescribed as requirements with respect to a health information network provider in the course of providing services to enable a health information custodian to use electronic means to collect, use, disclose, retain or dispose of personal health information:
>
> …
>
> . 5. The provider shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to,
>
> i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and
>
> ii. how the services may affect the privacy of the individuals who are the subject of the information

However, PIA is not obligatory for "health information custodians"[50] (yet see *infra*).

Ontario Regulation 331/11[51] made substantial changes to the original Regulation. With regard to eHealth Ontario,[52] an provincial agency tasked with facilitating the development of public electronic health record system that can qualify as HINP, a new Sec. 6.2 provides for PIA be conducted:

> (2) eHealth Ontario shall comply with the following requirements in creating or maintaining one or more electronic health records:
>
> …
>
> 6. It shall perform, for each electronic health record created or maintained, an assessment with respect to,
>
> i. threats, vulnerabilities and risks to the security and integrity of the personal health information contained in the electronic health record, and
>
> ii. how the electronic health record may affect the privacy of the individuals who are the subject of the information.
>
> 7. It shall
>
> i. make available to each health information custodian that provides personal health information to it for the purposes of creating or maintaining one or more electronic health records a written copy of the results of the assessment carried out under paragraph 6 for each record created or maintained for that custodian, and

[48] Ontario Regulation 329/04. http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_040329_e.htm

[49] Personal Health Information Protection Act, 2004, S.O. 2004, Ch. 3. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

[50] Definition of "health information custodian" is provided in Sec. 3(1) of PHIPA. As explained by IPC: "Examples of health information custodians in section 3(1) include a health care practitioner or a person who operates a group practice of health care practitioners that provide health care, hospitals, psychiatric facilities, long term care facilities, community care access corporations, pharmacies, laboratories, ambulance services and boards of health." Cf. http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf

[51] Ontario Regulation 331/11. http://www.lois-en-ligne.gouv.on.ca/html/source/regs/english/2011/elaws_src_regs_r11331_e.htm

[52] eHealth Ontario. http://www.ehealthontario.on.ca

ii. make available to the public a summary of the results of the assessments carried out under paragraph 6.

In August 2009, eHealth Ontario issued its PIA policy[53] which states:

> While eHealth Ontario is required to conduct PIAs under PHIPA when acting in its capacity as a HINP, as a matter of policy, the Agency will conduct privacy assessments wherever it undertakes a new or modified initiative involving a significant change in the way in which it handles Personal Information (PI) or Personal Health Information (PHI). In addition, eHealth Ontario will conduct PIAs on all ONE Products [network for sharing information]. Further, the results of such assessments will be provided to internal and/or external stakeholders, and identified privacy risks will be tracked and monitored for mitigation.

2. Guidance material

In October 2005, the Ontario Information and Privacy Commissioner has issued "*Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*."[54] The document explicitly states:

> The IPC understands that privacy impact assessments are not required under PHIPA for health information custodians. As such, health information custodians that use these guidelines to conduct a PIA will not be expected to submit their PIA to the IPC for review under PHIPA. However, the IPC may use any PIA as a starting point for any investigation into a breach of privacy under PHIPA (p. 4).
> The IPC recognizes that privacy impact assessments are not formally required under PHIPA, unless an organization is classified as a "health information network provider" (p. 8).
> … the IPC strongly recommends that health information custodians conduct a PIA on proposed or significant existing information systems, technologies or programs involving personal health information … even if they are not a health information network provider who is formally required to conduct a PIA under PHIPA (p. 9).

3.2.3 Alberta

1. PIA legal bases

Sec. 64 of the **Health Information Act**[55] is the main provision that requires PIA be conducted:

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

[53] *eHealth Ontario Privacy Impact Assessment Policy*, version 2. http://www.ehealthontario.on.ca/pdfs/Privacy/PrivacyImpactAssessmentPolicy.pdf
[54] Ontario Information and Privacy Commissioner, Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act. http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf
[55] Health Information Act, RSA 2000, c H-5. http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest

However, PIA must be also conducted in the following situations:

- disclosure to the Minister or the Department individually identifying health information [Sec. 46(1)]
- making prescribed health information accessible in Alberta Electronic Health Record (AEHR) [Sec. 56.3(3)]
- data matching by custodians or health information repository [Sec. 70(3)]
- data matching by custodian or health information repository and non-custodian [Sec. 71(2)].

Besides, under Sec. 84(1) the Information and Privacy Commissioner is empowered to:

> (f) comment on the implications for access to health information or for protection of health information of privacy impact assessments submitted to the Commissioner under section 46(5), 64, 70 or 71.

2. Guidance material

In 2010, the Office of the Information and Privacy Commissioner of Alberta (OIPC) has issued PIA guidance for the purposes of the Health Information Act.[56]

3.3 OPC AUDITS OF PIA PRACTICE

In June 2004, the TBS commissioned an independent mid-year review of a limited sample of departments to determine the impact of PIA policy in promoting privacy best practices. While remarking that there was evidence that the policy was having the desired effect of improving compliance with privacy legislation, the study also identified several problem areas.

The Office of the Privacy Commissioner is an ombudsman — an independent guardian of the privacy rights of Canadians. This role includes overseeing and enforcing two federal privacy statutes; the Privacy Act that applies to all federal government institutions, and the Personal Information Protection and Electronic Documents Act (PIPEDA) which extends personal data protection rights to the federally regulated private sector. The OPC is responsible for ensuring that the gathering and handling of personal information, in the public and private sectors, does not violate the privacy rights of Canadians. That means not only investigating and responding to complaints, but undertaking audits, conducting research into privacy issues, promoting public awareness and education, and providing advice to Parliament, government, and the private sector on privacy issues.[57]

The Office of the Privacy Commissioner has an audit and review function, and in late 2007, it published an audit report containing multiple recommendations for improvements.[58] As an Officer of Parliament, the Privacy Commissioner has the authority under the Privacy Act to examine the collection, use, disclosure, retention and disposal of personal information by

[56] Office of the Information and Privacy Commissioner of Alberta, *Privacy Impact Assessment Requirements for use with the Health Information Act*, 2010.
http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf
[57] Bloomfield, Stuart, "The Role of the Privacy Impact Assessment", Managing Government Information 2nd Annual Forum, Office of the Privacy Commissioner of Canada, Ottawa, 10 March 2004.
http://www.priv.gc.ca/speech/2004/sp-d_040310_e.cfm
[58] Privacy Commissioner of Canada, *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report, October 2007. http://www.priv.gc.ca/information/pub/ar-vr/pia_200710_e.cfm

government institutions. The TBS PIA Policy specified that the OPC was to receive notification of all privacy impact assessments, and may provide advice and guidance to institutions with respect to potential privacy risks.[59]

Five years after the TBS introduced its PIA policy in 2002, the OPC carried out an audit of government institutions' practice of PIA. The OPC found that some government institutions had made a serious effort to apply the policy, but that still more effort was required.[60]

It also found that "Present PIA reporting and notification standards provide little assurance or information to Canadians seeking to understand the privacy implications of using government services or programs. Only a minority of government institutions regularly post and update the results of PIA reports to their external Web sites, and when summaries are posted, they often fail to disclose the privacy impact of new modes of delivery (and how associated issues are being resolved)."[61]

The OPC said that there had been a general improvement in the level of rigor and professionalism brought to the preparation of PIAs since issuance of the TBS PIA policy.[62]

The OPC assessed nine government departments and institutions against four primary criteria. In addition to the detailed audit on these nine entities, the OPC conducted a survey of 47 additional institutions, asking each to self-assess against the same four evaluation criteria.[63] The four criteria were the main responsibilities of institutions vis-à-vis the PIA Policy and Guidelines, namely:

- To conduct PIAs, at the time of program or service design, for all new initiatives (or substantially redesigned programs and services) that may raise privacy risk;
- To provide a copy of the final PIA, approved by the Deputy Head, to the OPC, prior to implementing the initiative, program or service;
- To develop risk assessment and mitigating measures for privacy issues identified and to ensure that privacy mitigating measures are implemented; and
- To make PIA summaries public.

Although the OPC identified several examples of good practice, the audit found that federal institutions had been generally slow in implementing the PIA policy.[64] It found that PIAs suffered from common omissions and defects, many of which were the product of process-related weaknesses. In order to establish a benchmark for the evaluation of management control frameworks, the OPC developed a PIA process maturity model derived from the control objectives for information and related technology (COBIT). The maturity levels ranged from zero (non-existent) to 5 (optimised).[65] The model was used to measure each

[59] OPC, 2007, op. cit., pp. 7-8.
[60] OPC, 2007, op. cit., p. 4.
[61] OPC, 2007, op. cit., p. 4.
[62] Bloomfield, op. cit.
[63] Office of the Privacy Commissioner of Canada, *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report of the Privacy Commissioner of Canada, Ottawa, 2007, p. 9.
[64] Ibid., p. 10.
[65] The audit report describes (at p. 13) Level 5 thusly: "The assessment of operational privacy impacts has been integrated into the entity's overall risk management framework (at the center of which exists a formal PIA process). Organization wide controls ensure continuous and effective monitoring for compliance with the organization's own PIA process and the Treasury Board Policy. An individual / body is charged with overseeing compliance with the Policy and a body composed of senior personnel is charged with reviewing and approving PIA/PPIA candidates once complete. The organization conducts performance monitoring on key financial,

institution's PIA environment and to indicate the degree to which each entity was likely to comply with PIA policy. Only three of the nine institutions had well managed and measurable PIA environments. Of the 47 federal institutions polled, 89% of respondents indicated they actively used personal information in the delivery of programs and services, but 68% said they did not have a formal management framework in place to support the conduct of PIAs.[66]

The audit report said "the PIA process was far from being fully integrated into the overall risk management strategies of individual entities". The most common control weakness identified within the management systems reviewed was the lack of a mandatory and formal screening process for all programs, services, plans and policies to identify potential PIA candidates. Sixty-four per cent of respondents indicated that they did not have policies or processes in place to identify all activities requiring privacy impact analysis.[67]

Although the PIA requirements associated with a submission to the Treasury Board help to ensure that major, or soon-to-be-funded, proposals do not proceed without consideration of potential privacy impacts, the submission process does not provide sufficient coverage over program changes or the various micro-initiatives undertaken within large approved programs. These smaller initiatives or program changes, particularly when combined, can have serious privacy impacts, and should therefore be given consideration as potential PIA candidates.[68]

The OPC found little consideration provided for projects involving intra-, inter- or cross-jurisdictional flow of information or projects. In many such cases, accountability for PIA rests with more than one institution. As departmental programs and initiatives become increasingly integrated, and as data sharing activities within government become more commonplace, the risk of privacy breaches or improper personal information handling practices increases accordingly. [69]

The OPC noted numerous cases where PIAs were not initiated until well after a project's conception or design and that institutions were generally slow in addressing the identified privacy risks.[70] Institutions are obliged to make summaries of their PIAs available to the public in a timely manner, but the OPC found that only a minority of institutions were regularly posting and updating the results of PIA reports on their websites. The OPC commented that "one must question whether the current public disclosure standards are providing any value or comfort to the citizen seeking to understand the privacy implications of using a specific government service or program."[71] It also found that the quality of PIA summaries was generally poor.

The OPC did report some good news, however. Some departments did demonstrate good practices. One department held an annual conference for privacy officers from its headquarters and regional office to discuss privacy and PIA issues, and senior management awareness was fostered by frequent presentations to the department's management committee. Another had a privacy management framework committee comprising senior officials which met monthly to review and approve PIAs before submission to their Deputy

operational and human resource aspects of PIA operations, and the results of PIAs are integrated into ongoing project management."

[66] OPC, 2007, op. cit., pp. 11-12.
[67] Ibid., p. 14.
[68] OPC, 2007, p. 15.
[69] OPC, 2007, p. 16.
[70] OPC, 2007, p. 19.
[71] OPC, 2007, p. 20.

Minister for sign-off. Interestingly, one of the institutions with good practices was the Royal Canadian Mounted Police (RCMP).

In its recommendations, the OPC said that beyond having the necessary resource capacity to implement the PIA policy, the single most important determinant of success is the existence of a sound management control framework. It recommended that deputy heads of all government institutions should reaffirm their commitment to privacy protection and ensure that their organisation has an adequate administrative infrastructure to

- Identify and document all proposals that may present privacy risks;
- Establish a sound structure for organizational accountability;
- Develop and implement a system to track all proposals subject to the PIA policy, and the detailed PIAs conducted;
- Provide guidance and training to managers and staff; and
- Establish quality control, consultation, communication, follow-up and evaluation procedures for PIA.[72]

It recommended that federal institutions should seek to better integrate privacy analysis, including the need for PIAs, into their overall risk management.

The OPC noted a shortage of PIA personnel, such that government institutions were relying heavily on the professional services of external contractors and thus were less likely to develop the in-house capacity to conduct such assessments and may overlook some of the privacy risks of programs or plans that emerge from a sound understanding of the business processes and data flows unique to each organisation.[73]

It recommended more training and guidance be given to program managers to make them aware of their responsibilities under the PIA policy and to give them the knowledge and skills necessary to conduct PIAs.[74]

It recommended that the internal audit branches of all federal institutions should include privacy and PIA related reviews in their plans and priorities in the future. [75]

It saw a need for a federal privacy assessment registry, to provide a single window of access to PIAs across government. The registry could be used by the public to better understand the substance and privacy impacts of government projects and by institutions such as the Treasury Board Secretariat and the Privacy Commissioner to monitor PIA activities. [76]

It also saw a need to deal with the broader privacy implications of plans and policies that may not be easily addressed at the project or service level, something it termed a "strategic privacy impact assessment".[77] It raised concern about long-term changes that may occur to an individual's privacy, not only as a result of a single isolated action but also by the combined effects of each successive and interdependent intervention. Thus, the OPC recommended that the Treasury Board Secretariat should work with federal institutions to encourage the

[72] OPC, 2007, p. 22.
[73] OPC, 2007, p. 25.
[74] OPC, 2007, p. 26.
[75] OPC, 2007, p. 27.
[76] OPC, 2007, pp. 28-29.
[77] OPC, 2007, p. 30.

assessment of cumulative privacy effects likely to result from a program in combination with other projects or activities. [78]

The OPC commented that "enhancing the transparency of the privacy impact assessment process is critical to improving the quality of privacy analysis in government. Greater scrutiny generated by public exposure can prompt greater care in the preparation of PIAs and provide Parliament and the public with the necessary information to have more informed debates concerning privacy protection. Public disclosure may also provide additional assurance that privacy impacts are being appropriately considered in the development of programs, plans and policies – essentially holding each institution to account for the adequacy of the privacy analysis that was undertaken."[79]

The importance and value of privacy audits were demonstrated again when the OPC presented an audit report to Parliament in February 2009, which contained an audit of four government agencies which operate databases housing vast quantities of personal information. Commissioner Stoddart concluded that "The personal information of Canadian voters is not adequately protected."[80]

3.4 COMMENTS ON THE SHORTCOMINGS AND EFFICACY OF PIA IN CANADA BY PIA EXPERTS

Robin Bayley and Colin Bennett observe that

> Canadian PIAs seldom involve public consultation, opinion polling or other means of gauging the privacy values of the Canadian public. They tend to focus on legal compliance rather that doing the right thing and asking larger questions. Although most methodologies include guidance about considering these issues, the end product, and that which gets reviewed, tends to resemble a compliance checklist and does not require documentation of deliberations…. A related shortcoming relates to publicity. There is no common practice with regard to the publication of either the full PIAs or their summaries. Central PIA registers would overcome organisations not posting their PIA summaries, and allow organisations publicly to seek consultation. With regard to implementation, Canadian PIAs also fall short. The extent to which the PIAs are revisited and revised and the promised mitigation measures implemented is unknown. However, privacy regulators have reason to believe that PIA plans are not always carried out. The system would benefit from increased accountability for implementation of PIA plans. Currently, there is no reporting mechanism in Canada for the implementation of PIA plans. [81]

Bayley and Bennett say that Canadians would clearly benefit if more private sector organisations completed PIAs, to possibly stave off later complaints and investigations. The newer private sector privacy laws are generally more outcome or principles-based, so private sector organisations have more freedom to determine how they will comply. In no jurisdiction in Canada are PIAs mandatory in the private sector. Alberta is the exception in legislatively requiring PIAs to be conducted by "private" health-care organisations. For PIAs to be adopted by more companies, however, private sector organisations must know about PIA

[78] OPC, 2007, p. 31.
[79] OPC, 2007, p. 29.
[80] Office of the Privacy Commissioner of Canada, "Audit reveals privacy gaps at federal agencies", Press release, Ottawa, 12 Feb 2009. http://www.priv.gc.ca/media/nr-c/2009/nr-c_090212_e.cfm
[81] Bayley, Robin, and Colin J. Bennett, "Privacy impact assessments in Canada", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

methodologies, have tools that work for their organisations and believe that the benefits will outweigh the cost. They will likely conduct PIAs differently, or consider different risk management factors. Economic factors may outweigh compliance motivation, but market forces could mean that private organisations consider public perception and reputational risk as more important than their public counterparts.[82]

Reviews, rather than audits, are the norm in Canada. Reviews are an effective part of the PIA system in Canada and provide much additional value. Where reviews are not required or recommended, less formal, voluntary consultations may take place. PIAs are reviewed externally to the organisation in:

- BC, where the central agency reviews and "accepts" PIA reports on certain types of higher-risk and profile initiatives,
- Ontario, where the central agency reviews the Preliminary Analysis and some IT committees review reports,
- Alberta, where the privacy commissioner reviews and "accepts" PIA reports and
- Canada, where the privacy commissioner reviews, but does not accept or reject them.

Thus, a review may be conducted outside the organisation that conducted the PIA, but may still occur within government. Where an independent privacy commissioner reviews the PIA, the organisation may also have voluntarily shared the PIA and consulted with the central agency. Where there is no obligation to submit the PIA to the privacy commissioner, this may be done voluntarily for high-profile and novel initiatives that raise new issues because the privacy commissioner usually has the ability to comment publicly on programs.[83]

Generally in Canada, only PIA summaries are published (by posting on an organisation's website), and individuals wanting to see the entire PIA must apply under FOI legislation. Under that process, applicants may face delays of a month or more, fees and severing or redacting of information. Commonly, information relating to security controls would be withheld. Other exceptions to release relate to policy advice, legal privilege and executive confidence and harm to intergovernmental relations, international affairs and defence, law enforcement and financial, economic or third-party business interests. Jurisdictions have slightly different wording and precedents regarding the interpretation of these exceptions.

The timeliness of posting of summaries varies as does compliance with the basic requirement to publish and the descriptiveness of the summary. Of the jurisdictions studied, Ontario is the only one with no requirement to publish PIAs or summaries. The most fulsome summaries are provided by government of Canada public institutions but even those can be brief and do not generally confer a full understanding of the privacy issues and mitigation strategies. Most provincial summaries describe the initiative in a paragraph or two and serve only as a notice that a PIA has been completed. Exceptions exist and some organisations post entire PIAs or very detailed summaries.[84]

Ontario does not require PIAs or summaries to be published, although some may be found online, especially in the health sector. Unlike the other jurisdictions, the government of Ontario does not publish its new PIA tools online, but the Commissioner publishes her tools. It is difficult to see how the benefits of the methodology will spread to the private sector, when these models are not readily available.[85]

[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Ibid.

Roger Clarke has criticised the Treasury Board Secretariat's 2010 Directive because, he says, it has retreated from what was previously a broader conception of a PIA, such that all that is now required is a Data Protection Law Compliance Assessment. It has achieved this by creating the notion of a core PIA, which comprises "standardized elements of a PIA that are directly linked to policy and legal compliance". The guidance appears to exclude the affected public from the definition of stakeholders, and it fails to even mention the possibility of public consultation, although it does require some public reporting.[86]

He further comments that the Treasury Board's original documents required PIAs to "resolve privacy issues that may be of potential public concern", required "consultations with clients ... and other stakeholders", and appeared to encompass the affected public as part of the stakeholder definition.[87]

Under Alberta's HIA, "custodians" of personal health information must submit PIAs to the Information and Privacy Commissioner before implementing practices or information systems that will collect, use or disclose individually identifying health information. This includes changes to existing practices or information systems. PIAs submitted to the OIPC under the HIA must follow the format described in the PIA Requirements. The OIPC reviews the PIA and may raise questions about it, especially if impacts on privacy are significant or unmitigated or if the risks to privacy appear to outweigh the benefits of the project.[88]

An OPC official said that of the 90 PIAs his office had examined between May 2002 and March 2004, the most common omissions were the following:

- Failure to include a complete inventory of data elements collected and used (information may be described, but not itemized);
- Failure to describe adequately the business process;
- Failure to adequately describe the information security infrastructure associated with the project.
- Failure to include an action plan.[89]

The office of Jennifer Stoddart, Privacy Commissioner of Canada, carried out an audit of PIA practice in federal government institutions in 2007 and found, among other things, that

> Only a minority of the institutions we audited were regularly posting and updating the results of PIA reports to their external web sites. Of the nine entities audited, only four had made PIA summaries publicly available. Worse, in all but one of those four cases, the inventory of summaries available to the public was incomplete. Similarly, of the 47 federal institutions we surveyed, only 25 per cent of respondents indicated that PIA summaries were made accessible to the public through postings to their external websites. Further 50 per cent of respondents indicated that PIA summaries were not being published at all. Just as the public reporting on PIAs was lacking in completeness, so too was it lacking in quality. Despite the government's recommendation that PIA summaries describe the privacy impacts of all new programs and the measures taken to mitigate them, none of the departmental summaries we reviewed contained more than a simple project description and "privacy disclaimer". In many respects, the PIA summaries seemed more like communication tools than reports on substantive privacy concerns (and not for reasons pertaining to security, legal or confidentiality requirements). Privacy issues were rarely described and action plans were generally missing. One wonders whether the public

[86] Clarke, op. cit., 2011, p. 117.
[87] Clarke, op. cit., 2011, p. 118.
[88] OIPC, 2009, p. 5.
[89] Bloomfield, op. cit.

disclosure standards from 2002 (now revised) provided any value or comfort to a citizen seeking to understand the privacy implications of using a specific government service or program.[90]

3.5 BEST ELEMENTS

The governments of Canada, Ontario, BC and Alberta have all updated their primary PIA instruments in the last two years. Changes were made to address the ambiguity in previous requirements and common deficiencies in the level of detail in the appended documentation. Whether these more refined processes add up to better privacy protection for Canadians, however, is still an open question.[91]

Among the elements of PIA policy and practice in Canada that we most like are the following:

Treasury Board of Canada policy requires government institutions to develop and maintain privacy impact assessments for all new or modified programs and activities that involve the use of personal information.

It has developed PIA guidance documents, policies and directives and continues to update those.

The Privacy Act obliges government institutions to register all personal information banks with the Treasury Board.

The Treasury Board is obliged to review the manner in which PIBs are maintained and managed.

PIA is regarded as a component of risk management. Simple compliance with the Privacy Act is not enough. Government departments and agencies are expected to identify risks to privacy and to develop possible solutions for each risk and an action plan.

The directive ties PIAs with submissions to the Treasury Board for program approval and funding. This is one of the strongest features of Canadian PIA policy. Further the PIA has to be signed off by a senior official before submission to the Treasury Board. Department and agencies also have to provide a copy of the PIA to the Privacy Commissioner at the same time.

PIAs are to be initiated at the earliest possible phase of project planning.

The PIA Directive and Guidelines set criteria for when a PIA is to be initiated.

The Directive provides for the possibility of cross-jurisdictional PIAs.

The Treasury Board of Canada Secretariat has an oversight role, to monitor compliance with its Directive on Privacy Protection which also applies to PIA. However, the TBS does not approve PIAs; it only reviews them to ensure they are complete.

[90] Stoddart, Jennifer, "Auditing privacy impact assessments: the Canadian experience", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
[91] Bayley, Robin, and Colin J. Bennett, "Privacy impact assessments in Canada", in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

Although PIA is regarded as a process, the orientation of the Directive, Policy and PIA Guidelines is towards completing the PIA report. The PIA Guidelines and Directive set out what a PIA is expected to cover. The PIA is expected to identify risks to privacy and to categorise them using a numbered scale (with 1 representing the lowest level of potential risk to 4, the highest level).

The Guidelines recognise that different skill sets need to be brought together in order to carry out a PIA.

The Guidelines contain two questionnaires (the second is for cross-jurisdictional PIAs), the responses to which form the basis of the PIA report. The questions require more than a yes or no response. Respondents are to provide details further to their yes or no answers. The questions are based on privacy principles.

There seems to be a possibility of consultation with stakeholders, but little emphasis is placed on the possibility. More emphasis is placed on communicating the results of the PIA to the public.

Summaries of PIAs are to be posted on the department or agency's website, but the full report would be better.

The Guidelines identify several common privacy risks as well as potential outcomes of a PIA.

In 2003, the Treasury Board Secretariat published a report on PIA best practices.[92]

The government of Canada developed a PIA Audit Guide, "intended as a reference tool for Internal Auditors in the Government of Canada and may also be of assistance to the privacy community, including PIA Coordinators".

[92] Treasury Board Secretariat, Report on Best Practices Identified During the Implementation of the Privacy Impact Assessment Policy and Guidelines, Chief Information Officer Branch, 20 March 2003. http://www.tbs-sct.gc.ca/pgol-pged/pia-best/pia-best00-eng.asp

4 HONG KONG

4.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

Despite numerous calls by the Office of the Privacy Commissioner of Hong Kong for the use PIAs, the Office has not issued any formal guidance on how to conduct a PIA in Hong Kong.

In 2001, the Office published a document that included discussion of "strategic planning and privacy impact assessment", [1] but the guidance was minimal. It defined a PIA as a systematic process that evaluates proposed initiatives or strategic options in term of their impact upon privacy. The purpose of a PIA is to identify a project or proposal's potential effects upon privacy, and examine how detrimental effects might be mitigated. The document stated that the PIA needs to commence at the outset of any initiative, should begin with the definition of the problem or statement of issues, that there are advantages to outsourcing PIAs, that they may be critical in influencing consumer or public opinion. Importantly, the 2001 document recommends that the outcome of any PIA should be measured against the influence it exerts on the original plans and policies, with the goal that decision-makers work towards decisions that are privacy-enhancing.

While PIAs were mentioned many times in the years following that document, it was only in 2010 that the Office of the Privacy Commissioner released more detailed information. In July 2010, the Office released a three-page 'Information Leaflet' on PIAs, recommending that a PIA process should include the following components[2]:

1. Data processing cycle analysis – this stage involves a critical review of the purpose and rationale behind the project in deciding whether it is necessary to collect the kind, amount and extent of personal data contemplated by the data user. It then goes on to list and discuss the six data protection principles.

2. Privacy risks analysis – the relevant factors that data users should take into account include:
   - The functions and activities of data users;
   - The nature of the personal data involved;
   - The number of individuals affected;
   - The gravity of harm that data subjects may incur should their personal data be improperly handled;
   - The privacy standards and rules prescribed under applicable codes of practices, policies and practices that the data users should observe, etc.

3. Avoiding or mitigating privacy risks.
   It is highly advisable that a "privacy-by-design" approach be adopted and privacy enhancing technologies be considered and used in the design stage of the personal data system. The aim of such measures is:
   - To reduce the amount of personal data collected;

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

[2] Office of the Privacy Commissioner for Personal Data, Hong Kong, Information Leaflet, July 2010. http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf

- To safely delete personal data when no longer required for the project;
- To define clearly and limit the number of persons who can access the personal data on a "need-to-know" basis. A data user may find it justifiable to use a role-based approach in assigning and reviewing the access right to be given to its employees and agents;
- To incorporate an appropriate level of security measures in the system, so that confidentiality, integrity, and accountability can be achieved. In particular, an organisation should have logging and reporting mechanisms to detect and notify appropriate parties in the event of a data breach;
- To promulgate a clear and easy-to-understand privacy policy that can be effectively communicated to data subjects and stakeholders to promote transparency;
- To consult data subjects and stakeholders when a project of significant privacy impact is to be introduced.

4. PIA reporting – the findings, recommendations and privacy protective measures should be clearly reported and documented. As a PIA report documents the due process undertaken by the data user to proactively manage privacy risks, a PIA report will not only serve as a benchmark for future audits and reviews but can often provide useful information to the Privacy Commissioner's consideration if a complaint comes before him. It may also be useful if PIA on projects of great public concern are published. The contents of a PIA report may include the following:
   - Description of the project;
   - The data processing cycle analysis;
   - The identification of the privacy risks;
   - The way and means used to address these calculated risks and an explanation of less privacy intrusive alternatives considered and where appropriate, why they have been adopted.

4.2 LEGAL BASIS

The six data protection principles contained in the Personal Data (Privacy) Ordinance of 1996 lay down the legal requirements to be observed by data users in handling the different aspects of the data processing cycle from collection, accuracy, retention, use, security, access rules and data correction.[3]

The Ordinance itself does not include any language about PIAs, and there are no powers for the Commissioner to require PIAs to be carried out on potentially privacy-invasive systems.[4] There are components of the Ordinance, however, that could be complemented by a PIA. For example, under section 8(1)(d), the Commissioner has a duty to examine proposed legislation that may affect data privacy and report the results of his examination to the relevant agencies.[5]

[3] http://www.pco.org.hk/ord/ord_a.html#principles

[4] Greenleaf, Graham, D. Korff, Ian Brown et al., *Final Report of the Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, European Commission Directorate-General Justice, Freedom and Security, May 2010, section B.3 on Hong Kong, p. 33.

[5] Clarke, Roger, Appendix G on Hong Kong as part of *Privacy Impact Assessments: International Study of their Application and Effects*, prepared for the Information Commissioner's Office, Wilmslow, UK, October 2007.

Considering the lack of an explicit power to order PIAs, and with the possibility of an implicit power to consider PIAs, the Privacy Commissioner of Hong Kong has a history of suggesting that PIAs be undertaken for specific initiatives. The Commissioner has also produced guidance that describes circumstances in which the Office recommends the completion of PIAs.[6] The Commissioner has also been including the language of "assessment" in his messages to data controllers.

In 2000, the Commissioner recommended for the first time that PIA be conducted for both the new ID and electronic heath systems. In turn, the Hong Kong ID card was the subject of PIAs on four occasions between 2000 and 2004, but we have been unable to find any PIAs for electronic health systems.

In 2001, the Commissioner issued limited guidance on e-Business, which included a recommendation that both private and public sectors adopt PIA as standard practice, as a means of introducing impartiality to a review process and as part of the public consultation exercise.[7] By 2003, the Commissioner began calling for education programmes for PIAs, seeing them as "a strong contribution to privacy compliance".[8] In 2004, the Commissioner exercised powers under section 8(5) of the Ordinance to issue a guideline document for employers on workplace surveillance. In this Guidance document,[9] the Commission introduced "the 3 A's concept", that is, assessment, alternatives and accountability for the employer to take into account before deciding whether to engage in any employee monitoring activity.

In 2005, the Commissioner began promoting the use of PIA as a way to "plug the loopholes likely to contravene the requirements of the Personal Data (Privacy) Ordinance".[10]

There are no records or statistics of the number of PIAs that have been undertaken in Hong Kong.[11] There have been some mentions of PIAs for caller number display, electronic road pricing, a "speed map panel",[12] and online banking services, but the PIAs have not been publicly released. In 2008, the Commissioner recommended that both the Hong Kong Hospital Authority and the Food and Health Bureau conduct PIAs. The Commissioner also expected that the Office would conduct a privacy impact assessment and then a "privacy compliance audit" in respect of the Electronic Health Record Sharing Programme, though this would likely take more than five years from early 2010.[13]

By 2010, the Office of the Commissioner released an information leaflet on PIAs, claiming that PIAs had "become a widespread privacy compliance tool" and advised data users to adopt PIAs. The Commissioner stated clearly that the "PIA is not a substitute for the legal

[6] Linden Consulting, *Privacy Impact Assessments: International Study of their Application and Effects*, prepared for the Information Commissioner's Office, October 2007, p. 13.
[7] 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, section 8.5, 2001. http://www.pcpd.org.hk/english/publications/eprivacy_9.html
[8] Office of the Privacy Commissioner for Personal Data, Annual Report for 2003-04. http://www.pcpd.org.hk/english/publications/overview2004_1.html.
[9] Privacy Guidelines: Monitoring and Personal Data Privacy at Work in December 2004
[10] http://www.pcpd.org.hk/english/infocentre/press_20050901.html
[11] Waters, Nigel, Privacy Impact Assessment from an International Perspective, University of New South Wales Faculty of Law Research Series, UNSWLRS 65, 2010.
[12] Woo, Roderick B., "The Work Report of the Privacy Commissioner", Office of the Privacy Commissioner of Hong Kong, December 2009, p. 42.
[13] Ibid., p. 77.

protection available to data subjects under the Ordinance." Rather, the PIA report can provide useful information for the Commissioner's consideration when a complaint comes before him.

Despite all of this activity, there is still no strict legal obligation for a PIA. In a review of the Hong Kong law, initiated by the Office of the Privacy Commissioner in 2006, the role of PIAs was not addressed. Similarly, in a government review of the Ordinance in 2010, there was again no reference to PIAs.

4.3 COMMENTS ON THE SHORTCOMINGS AND EFFICACY OF PIA IN HONG KONG BY PIA EXPERTS

The two most significant shortcomings in Hong Kong's use of PIAs is that the Ordinance does not even make reference to PIAs, and the Office of the Privacy Commissioner has not issued guidance on how to conduct PIAs, apart from an informational three-page leaflet. As a result, the Commissioner cannot order PIAs, and has not prescribed the nature of PIAs in Hong Kong. Additional shortcomings include: any PIA framework developed by the Commissioner could only focus on adherence to the data protection principles because of the limited remit of the Office under the Ordinance,[14] and that the information leaflet only makes mention of the *possibility* of publishing PIAs (the limited number of published PIAs for review is perhaps a complementary problem).

The lack of published PIAs makes it very difficult to assess the state of PIAs in Hong Kong. We tried to find publicly available PIAs but unfortunately the results were limited to a single initiative: a number of PIAs were conducted as part of the introduction of a new "smart" identity card (SMARTIC) in the late 1990s and early 2000s.

An author of one of these PIAs, Nigel Waters, has since reviewed all of the PIAs conducted on the smartcard project in order to analyse the advantages and drawbacks of PIA in Hong Kong.

Some of the main drawbacks identified in a report by Nigel Waters[15] include:

- The Immigration Department delayed publication of the full PIAs. They were often delayed for months, and one PIA, from some time between 2002 and 2004 remains unpublished.
- The PIAs could not limit expansion of uses. That is, despite recommendations to avoid function creep, the policies surrounding the system (though not necessarily immediately related to the system) were changed to expand the use of the system for multiple non-immigration uses.
- The later-staged PIAs focussed attention on detailed systems design and procedural safeguards, rather than considering "big picture" issues, such as justification for privacy intrusion, alternatives and risk of function creep, that is possible and justifiable at earlier stages.
- Once key decisions on project scope and design have been made, it is unreasonable to expect PIA assessors to revisit issues that have been effectively closed through the political process.

[14] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, February 2011, pp. 111-120.
[15] http://law.bepress.com/cgi/viewcontent.cgi?article=1260&context=unswwps

- Where the assessor is funded by the project proponent, the pressure on him or her means that the PIA will only hint at potential problems although clues as to less privacy invasive alternatives can be included for the more experienced readers. The risk associated with this strategy is that regulators and policy makers can still miss those clues.
- Despite project proponents' initial commitment to implementing PIA recommendations, it is all too easy for the initial commitment to be either partially or wholly abandoned at a later stage. Privacy regulators must thus be more active in following up on PIA reports and their implementation.
- All interested parties should develop a more sophisticated understanding of the political and practical realities and take these into account when commissioning, producing or using PIA reports.
- PIA will not generally lead to better privacy outcomes if unaided.
- Even now, very few PIA reports are made public and when they are, this often happens too late for any meaningful policy shift or amendment to take place.
- The regulator must become more active in following up on PIA reports, asking if recommendations were accepted or refused and for explanations.

4.4 BEST ELEMENTS

We have identified the following good elements in Hong Kong's PIA practice:

- The three-page leaflet from the Office of the Commissioner is somewhat limited, but it does include a statement that organisations should "consult the data subjects and stakeholders" in the process of conducting a PIA.
- PIA is regarded as a process.
- PIA should commence at the outset of an initiative.
- The outcome of a PIA should be measured against its influence on a project.
- A PIA report should serve as a benchmark for future audits.
- The Hong Kong Privacy Commissioner encourages of the PIA report.
- PIAs should be undertaken in both the public and private sectors.
- PIAs are regarded as a way to ensure accountability.

5 IRELAND

5.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

The Health Information and Quality Authority is an independent authority, established under the Health Act 2007, to drive improvement in Ireland's health and social care services. It has statutory responsibility for setting standards, monitoring healthcare quality, technology assessment and health information. It aims to ensure that service users' interests are protected, including their right to privacy, confidentiality and security of their personal health information. In this context, the Authority produced a PIA Guidance in December 2010.[1]

It says the primary purpose in undertaking a privacy impact assessment is to protect the rights of service users. PIA is a process that facilitates the protection and enhancement of the privacy of individuals. Another key benefit of PIAs is the value and cost savings they can bring to health and social care projects. A PIA is most beneficial when it is conducted in the early stages of a project. If it is conducted early, the outcome of the PIA can influence the development of a project before any significant investment has been made. The cost of risk mitigation at the planning stage of a project will be considerably less than the costs that could be incurred should changes be required to a project following implementation.

The PIA process begins at the planning stage of any new or significantly amended programme, initiative, system or project that involves the collection, use or disclosure of personal information. The process involves the evaluation of broad privacy implications of projects and relevant legislative compliance. Where potential privacy risks are identified, a search is undertaken, **in consultation with stakeholders**, for ways to avoid or mitigate these risks.

The collection, use, storage and disclosure of personal health information is necessary to the provision of effective health and social care. However, this can present significant risks to the privacy of the individual especially as ever-increasing amounts of personal health information are processed. Service providers must assess possible privacy risks in relation to the collection, use, storage and disclosure of personal health information at the planning stage of projects. By identifying any significant risks to privacy posed by a new initiative, it should be possible to mitigate or reduce these risks without necessarily impacting negatively on the success of the initiative. It will also drive an initiative to clearly identify what precise data are required and for what purpose, which will assist in focusing resources.

Conducting PIAs should be embedded as part of the project management framework so that the management of privacy risk is an ongoing process. Therefore, the PIA should be reviewed and updated throughout the duration of the project.[2]

The Authority has published an international review of PIA practice in other jurisdictions.[3] The review revealed that the countries studied have been heavily influenced by each other and have modelled their processes and guidelines on international practices. There is therefore a growing convergence in respect of what constitutes best practice in relation to PIAs.

[1] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010. http://www.hiqa.ie/resource-centre/professionals
[2] Ibid., p. 13.
[3] Health Information and Quality Authority, *International Review of Privacy Impact Assessments,* 2010. http://www.hiqa.ie/standards/information-governance/health-information-governance

The Guidance identifies the following benefits of undertaking PIAs:

- Service providers who undertake PIAs appropriately demonstrate that the privacy of individuals is a priority for their organisation. This helps to build the trust of the service user in the provider
- PIAs educate service providers about privacy and the rights of the service users.
- Service providers can potentially save money by conducting a PIA in the early stages of planning an initiative. Potential privacy risks or issues are much simpler to resolve prior to any significant investment being made.
- A clear focus will emerge as to the precise data required for an initiative.
- In the event of an unavoidable privacy risk or breach occurring, the PIA report can provide evidence that the service provider acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any negative publicity and loss of reputation. [4]

A PIA in its own right may not highlight all privacy risks or issues associated with an initiative. A PIA is a tool; it is dependent on service providers having the correct processes in place to carry out the PIA. These include identification of the correct stakeholders for the assessment, selection of those with the necessary knowledge and skills to carry out the PIA and involvement of senior managers in order to implement the PIA recommendations. It is essential that the PIA is regularly updated to reflect any changes to the direction of the initiative to ensure that all discoverable privacy issues are addressed.[5]

As the concept of conducting PIAs is new to the Irish health and social care sector, a sample PIA report based on this guidance has been developed and is available on the Authority's website for illustrative purposes (www.hiqa.ie).

Who should conduct a PIA?

The PIA should generally be undertaken by the project team. It may, however, be appropriate to consult service users as part of the PIA process. The service provider is ultimately responsible for the completion of the PIA and for implementing any changes to the project plan following recommendations from the PIA. PIAs should be reviewed and approved at a senior level with each PIA report being quality assured by senior management.

Like the Alberta PIA Requirements, the Irish Guidance says that if a PIA is conducted too early, the results will be vague as there may not be enough information available about the project, its scope and proposed information flows to properly consider the privacy implications and as such the PIA may need to be revisited. The PIA process should be undertaken when a project proposal is in place but before any significant progress or investment has been made. The findings and recommendations of the PIA should influence the final detail and design of the project. Conducting PIAs should be embedded as part of the project management framework so that the management of privacy risk is an ongoing process. The PIA should evolve in line with changes to the project.[6]

The PIA process

[4] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010, p. 14.
[5] Ibid., p. 14.
[6] Ibid., p. 18.

The Guidance identifies four stages in the PIA process as follows:
- Stage 1 – PIA threshold assessment
- Stage 2 – Identification of risks
- Stage 3 – Addressing the risks
- Stage 4 – the PIA report.[7]

Stage 1 – PIA threshold assessment

A service provider should routinely undertake a threshold assessment for every new health information project as well as proposals to amend existing information systems, sources or processes. A threshold assessment is a brief, initial assessment of a project, to determine whether its potential privacy impact necessitates a PIA. The threshold assessment consists of a checklist of 11 questions (detailed in Appendix 1 of the Guidance). If the answer to one or more of the questions is "yes", then a PIA is necessary. If the answer to all of the questions is "no", it will not be necessary. In either case, the completed threshold assessment should be signed and approved by the project lead and senior management.

Stage 2 – Identification of risks

Stage 2 involves identifying potential privacy risks through defining how the organisation manages privacy and exploring the project's scope, information flows and security arrangements. The service provider should document and explore the following:
- privacy management
- a description of the project
- the project type and stage of development
- the scope of the project
- the information flows.

Privacy management is how the service provider manages the privacy of personal health within the organisation. The PIA should examine information governance issues such as data protection and confidentiality, staff awareness of privacy policies, education and training of staff, and accountability for the handling of personal information. The service provider will generally need to review and update this section regularly. The Guidance suggests some questions:
- Is there a privacy policy in place that outlines the safeguards employed to protect service users' privacy and confidentiality?
- Is there a statement of information practices setting out the types of information collected, how it is used, if it is shared and how service users can access information held about them?
- Is the service provider compliant with the principles of data protection in legislation? Is the service provider the legal data controller for all personal data within the scope of the initiative?
- Is there a records management policy in place that includes a retention and destruction schedule? This should outline for how long particular types of information are held and the process for the secure disposal of both paper and electronic records.

[7] Ibid., p. 18.

- Are administrative, technical and physical safeguards in place to protect personal health information against theft, loss, unauthorised use or disclosure and unauthorised copying, modification or disposal?
- Is there an appointed privacy or information governance contact person?
- Is there a privacy breach management action plan in place?
- Are employees or agents with access to personal health information provided with training related to privacy protection and confidentiality requirements?

A description of the project

The project team should provide a description of the project including the reasons for undertaking it and address the following:

- details of the service provider or individual proposing the project
- the overall aims of the project (including how it ties in with the service provider's functions or activities)
- the drivers for or reasons behind the project
- the scope or extent of the project (whether it is national, regional or local)
- any links with existing projects or programmes.

The project type and the stage of development

The PIA should document the project type and stage of development. If a project is at a conceptual stage, all of the information needed for the PIA may not yet be available, e.g., the project team may not yet precisely know what the information flows will be or to whom it will be necessary to disclose information. Hence, the PIA will need to be revisited and updated as the project develops and decisions are taken. This section should address questions such as:

- Is this a new project?
- Is this an alteration or an addition to an existing project?
- What is the stage of development of the project?

The scope of the project

The PIA should examine the extent to which a project involves the collection, use or disclosure of personal information. This section looks at indicators such as the proportion of the population impacted by the project and the likely effects of the project on individuals. Generally, the greater the scope of the project, the more detailed the PIA will likely be. This section should address questions such as:

- What information is to be collected?
- Outline why each element of the data set is necessary.
- Are users aware of the proposed collection, use and disclosure of their personal information? Identify and describe what information is given and how it is given.
- Have users consented to use of their personal information? Does the project comply with the consent requirements of data protection legislation? Describe the consent process.
- Identify and describe:
  - All uses of the personal information.
  - How these uses relate to the purpose for which the information was collected.
  - Any changes to the purpose for using the information after it is collected.
  - Measures in place to prevent use for other purposes.

- Identify and describe any potential sharing of the information and how the user has been informed of this possibility.
- Will the information be linked or matched with an existing or proposed system? If yes, provide details.
- Does the project, system or initiative involve assigning or using an identifier or using an existing identifier for a new purpose? If yes, provide details.

The service provider should highlight any privacy risks in relation to each of the answers provided.

Information flows

The PIA should map the flow of information from the time it is collected, through its use and possible disclosure. It should address questions about how personal health information will be handled and used, the purpose for its collection, methods of disclosure and safeguards in place to protect privacy. Sample questions to identify potential risk for the information flows are:

- How is the information to be collected?
- What are the proposed uses of the information?
- Will the information be disclosed? To whom? What precautions are in place to prevent inappropriate disclosure?
- Will the data subjects have access to the information and the opportunity to correct any erroneous information?
- What security measures will be taken to protect the information from loss, unauthorised access, use, modification, disclosure or other misuse, including how data is transferred from sites or systems?
- Identify and describe the retention and destruction practices to be employed in the project.

Stage 3 – Addressing the risks

This stage in the PIA process involves an assessment of risks to individuals' personal health information and how best to mitigate or avoid them. In some cases, it may be necessary to balance the risks to privacy of personal information against the public good while having regard to legal requirements. This may require consultation with stakeholders affected, including the general public.

Analyse the risks

Risk analysis is a systematic process to understand the nature and to deduce the level of risk. In analysing the risks, it is necessary to determine the consequences and likelihood of a particular event occurring, thereby determining the level of risk. Analysing risks is not a one-off exercise; it is part of a process that should be repeated whenever there is a change in the circumstances that affect a risk. Sample questions for this stage of the PIA include:

- If the event were to occur, what is the likely impact on the service user?
- If the event were to occur, what is the likely impact on the service provider?
- What is the likelihood of the event occurring?

One approach to analysing risks is through the use of a risk matrix – a tool for ranking and displaying risks by defining ranges for consequences and likelihood.

Addressing the risks

The next step is to identify ways to reduce or eliminate the possibility of each risk occurring. The positive impacts of risk elimination should be balanced against how the goals of the project will be affected. Selecting the most appropriate option involves balancing the costs of implementing this option against the benefits derived from it. In each case, the cost of mitigating a risk should be appropriate and proportionate to the value gained in terms of protection of personal health information.

The cost of risk mitigation at the planning stage of a project is likely to be considerably less than the possible costs that could be incurred should changes be required to a project following implementation. Examples of proposed actions include:

- do nothing about the risk
- abandon the project completely
- amend the proposed project such that the risk is entirely removed
- remove an aspect of the risk, thereby reducing its possible impact
- employ security measures such as encryption or role-based access controls to address security concerns
- introduce an opt-out mechanism to allow individuals not to have their personal health information processed or included in the system, thereby eliminating the risk to their data
- a combination of the above.

These actions, and potentially others, and the consequences for both the individual and the proposed project should be considered and discussed in respect of each risk. The project manager should explain the option(s) chosen for each risk and the reasoning behind the choices. The actions proposed and approved by senior management should be monitored as the project evolves. If there is a residual or remaining risk, which cannot be mitigated, the project team must decide whether or not it is acceptable to continue with the project. Any residual risks should be documented in the service provider's risk register, which should be reviewed, updated and managed on a regular basis by the project team and the senior management.

Consultation with stakeholders and members of the public about the privacy risks associated with the project can prove valuable. Consultation can help in discovering the impacts of some privacy risks. Consultation is a way to gather fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks. Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report.

Stage 4 - the PIA report

According to the Authority, the final output of a PIA is a report which details the proposed project, the steps that were undertaken as part of the PIA process and any subsequent recommendations. The publication of PIA reports builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information.

Benefits of preparing and publishing a PIA report include:

- showing accountability in demonstrating that the PIA process was performed appropriately;
- enabling the experience gained and lessons learned throughout the process to be shared both within and outside of the service provider's organisation;

- empowering service users to inform themselves of the way their information is being used and the safeguards to protect it;
- demonstrating to the public that their privacy has been given due consideration, thereby improving public trust and confidence in the service provider.

The report should convey the following:
- a detailed description of the project including the objectives and justification for the project
- an overview of the PIA process
- the threshold assessment form
- an overview of the PIA process, its scope and the project's information flows
- a description of the specific risks identified
- a discussion of alternatives considered to mitigate or avoid these risks and a rationale for the decisions made
- a description of the privacy design features adopted to safeguard privacy
- details of any consultation with stakeholders, users or the general public
- an outline of any remaining risks and a business case justifying them and implications for the public or service users.

The focus of a PIA report should be on the needs and rights of individuals whose personal health information is collected, used or disclosed. Completed PIA reports should be published and presented in a reader-friendly format. The PIA report should be approved by senior management, as a measure for increasing accountability.[8]

5.2 LEGAL BASIS

1. General framework for privacy and data protection

Being a member of the Council of Europe, Ireland ratified the ECHR and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) and its Additional Protocol (ETS 181). Being a member of the EU, Ireland is bound by the Charter of Fundamental Rights and the EU data protection framework (see *supra*).

Arts. 40-44 of the Irish Constitution (1937) provide for the fundamental rights protection. However, the Constitution does not explicitly refer to the protection of **privacy**. According to the Irish Supreme Court, an individual may invoke Art. 40(3)(1) to establish an implied right to privacy: "*the State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen*."[9] The European Convention of Human Rights Act, 2003 gave further effect of the ECHR in Irish law.

The basic data protection legal instruments in Ireland are the **Data Protection Act, 1988**[10] that was substantially amended by the **Data Protection (Amendment) Act, 2003**,[11] and the

[8] Authority, pp. 17-32.
[9] Privacy International, *Privacy and Human Rights 2006. Country Reports – Republic of Ireland*, 2007. https://www.privacyinternational.org/article/phr2006-republic-ireland.
[10] Data Protection Act, 1988, No. 25 of 1988, http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html (official source).
[11] Data Protection (Amendment) Act 2003, No. 6 of 2003. http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html

European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.[12] The Office of the Data Protection Commissioner[13] is established under the Data Protection Act (Sec. 9).

2. Laws on PIA forerunners

In the implementation of the 1995 Data Protection Directive, sec. 13 of the Data Protection (Amendment) Act, 2003 added to the original Act a section dealing with **prior checking** (Sec. 12A):

> (1) This section applies to any processing that is of a prescribed description, being processing that appears to the Commissioner to be particularly likely –
> (a) to cause substantial damage or substantial distress to data subjects, or
> (b) otherwise significantly to prejudice the rights and freedoms of data subjects.
>
> (2) The Commissioner, on receiving –
> (a) an application under section 17 of this Act by a person to whom section 16 of this Act applies for registration in the register and any prescribed information and any other information that he or she may require, or
> (b) a request from a data controller in that behalf,
> shall consider and determine –
> (i) whether any of the processing to which the application or request relates is processing to which this section applies,
> (ii) if it does, whether the processing to which this section applies is likely to comply with the provisions of this Act.
>
> (3) Subject to subsection (4) of this section, the Commissioner shall, within the period of 90 days from the day on which he or she receives an application or a request referred to in subsection (2) of this section, serve a notice on the data controller concerned stating the extent to which, in the opinion of the Commissioner, the proposed processing is likely or unlikely to comply with the provisions of this Act.
> …
>
> (6) Processing to which this section applies shall not be carried on unless –
> (…)
> (c) (i) the period of 90 days from the date of the receipt of the application or request referred to in subsection (3) of this section (or that period as extended under subsections (4) and (5) of this section or either of them) has elapsed without the receipt by the data controller of a notice under the said subsection (3), or
> (ii) the data controller has received a notice under the said subsection (3) stating that the particular processing proposed to be carried on is likely to comply with the provisions of this Act, or
> (iii) the data controller –
> (I) has received a notice under the said subsection (3) stating that, if the requirements specified by the Commissioner (which he or she is hereby authorised to specify) and appended to the notice are complied with by the data controller, the processing proposed to be carried on is likely to comply with the provisions of this Act, and
> (II) has complied with those requirements.
>
> (7) A person who contravenes subsection (6) of this section shall be guilty of an offence.

[12] European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003, S.I. No. 535 of 2003. http://www.irishstatutebook.ie/2003/en/si/0535.html
[13] Office of the Data Protection Commissioner. http://dataprotection.ie

(8) An appeal against a notice under subsection (3) of this section or a requirement appended to the notice may be made to and heard and determined by the Court under section 26 of this Act and that section shall apply as if such a notice and such a requirement were specified in subsection (1) of the said section 26.

(10) A data controller shall pay to the Commissioner such fee (if any) as may be prescribed in respect of the consideration by the Commissioner (…)

(11) In this section a reference to a data controller includes a reference to a data processor.

3. PIA legal bases

No explicit basis for PIA in the laws of Ireland has been found.

Under Sec. (8)(1) the **Health Act, 2007**, the Health Information and Quality Authority (HIQA) has responsibility:

(i) to evaluate available information respecting the services and the health and welfare of the population;
(j) to provide advice and make recommendations to the Minister and the Executive about deficiencies identified by the Authority in respect of the information referred to in paragraph (i);
(k) to set standards as the Authority considers appropriate for the Executive and service providers respecting data and information in their possession in relation to services and the health and welfare of the population.

These provisions, especially paragraph (k), constituted a basis to issue a PIA guidance material for the health sector in Ireland (see *infra*).

4. Guidance material

For the purposes of the Irish public health and social care sector, in 2010 the Health Information and Quality Authority published a guidance on PIA in health and social care. The guidance is supported a PIA threshold assessment form and a sample PIA report. [14]

The Data Protection Commissioner has recommends a PIA be conducted if a biometric system is installed in a workplace:[15]

8. Before an employer installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out

or in a school, a college or other educational establishment:[16]

8. Before a school or college installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out.

[14] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, 2010. http://www.hiqa.ie/resource-centre/professionals/privacy-impact-assessments.
[15] Data Protection Commissioner, *Biometrics in the workplace.* http://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm
[16] Data Protection Commissioner, *Biometrics in Schools, Colleges and other Educational Institutions.* http://www.dataprotection.ie/docs/Biometrics_in_Schools,_Colleges_and_other_Educational_Instit/409.htm

5. Proposals

In Ireland, since 2008, the debate on the proposed Health Information Bill catches a lot of media attention. Public consultations have been conducted.[17] In January 2011, Prof. Jane Grimson, Director of Health Information at HIQA, told the Irish Medial Times that the Bill would include a requirement to conduct PIA:[18]

> HIQA will be setting standards in the broad areas of information governance, which would include a requirement to do a PIA in the future for a new project or projects to which there is major change to an existing system.

5.3 BEST ELEMENTS

The elements of the Irish *Guidance on Privacy Impact Assessment in Health and Social Care* that we most like and would recommend for a European PIA guidance include the following:

The Guidance regards PIA as a process that should be conducted most beneficially in the early stages of a project. The findings and recommendations of the PIA should influence the final detail and design of the project.

The Health Information and Quality Authority recognises that a PIA in its own right may not highlight all privacy risks or issues associated with an initiative. It says a PIA is a tool dependent on service providers having the correct processes in place to carry out the PIA. These include identification of the correct stakeholders for the assessment, selection of those with the necessary knowledge and skills to carry out the PIA and involvement of senior managers in order to implement the PIA recommendations.

The Guidance encourages consultation with stakeholders and members of the public to help discover the impacts of privacy risks, to gather fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks. Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report.

PIAs should be embedded as part of the project management framework. Therefore, the PIA should be reviewed and updated throughout the duration of the project.

The Guidance identifies benefits of undertaking PIAs.

The Health Information and Quality Authority has developed a sample PIA report based on its Guidance to help assessors.

The PIA should be reviewed and approved at a senior level with each PIA report being quality assured by senior management.

Service providers should routinely undertake a threshold assessment for every new health information project as well as proposals to amend existing information systems, sources or processes to determine whether its potential privacy impact necessitates a PIA.

[17] Department of Health, Proposed Health Information Bill. http://www.dohc.ie/issues/hib.
[18] Irish Medical Times, *Assessing the impact on privacy*, 10 January 2011. http://www.imt.ie/features-opinion/2011/01/assessing-the-impact-on-privacy.html.

The Guidance sets out in detail its PIA process. It suggests some questions to guide the process.

The Guidance encourages publication of the PIA report and says that doing so builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information.

The focus of a PIA report should be on the needs and rights of individuals whose personal health information is collected, used or disclosed.

6 NEW ZEALAND

6.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

The origins of privacy impact assessment in New Zealand date back to at least 1993, to the legislative requirement under section 98 of the Privacy Act 1993[1] to undertake Information Matching Privacy Impact Assessments (IMPIAs).[2] IMPIAs are legally mandatory assessments involving an examination of legislative proposals that provide for the collection or disclosure of personal information and used for an information-matching programme[3] in terms of the information-matching guidelines.[4] The Office of the Privacy Commissioner (OPC) issued guidance on their implementation in 1999.[5]

The New Zealand Privacy Commissioner plays a key role in monitoring IMPIAs and other PIAs.[6]

6.2 THE NEW ZEALAND PRIVACY COMMISSIONER'S GUIDE

The OPC published a PIA Handbook[7] in October 2002[8] (reprinted in 2007).[9] The Handbook defines a PIA as a "systematic process for evaluating a proposal in terms of its impact upon privacy", which can help an agency to identify the potential effects of a proposal on individual privacy, examine how any detrimental privacy effects can be overcome and ensure that new projects comply with the information privacy principles. A PIA is thus, a "valuable tool for businesses and governments which take privacy seriously".[10]

The Handbook, intended for people with the organisational responsibility for complying with data protection and privacy laws and policies, aims (p. 5):

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

---

[1] Superseding the Privacy Commissioner Act 1991.
[2] For contents of IMPIAs, see Office of the Privacy Commissioner, Guidance Note for Departments Seeking Legislative Provision for Information Matching, 16 May 2008, Appendix B. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching/#appendix
[3] See Office of the Privacy Commissioner, Operating programmes, 30 June 2010. http://privacy.org.nz/operating-programmes/
[4] Set out in section 98 of the Privacy Act 1993.
[5] Office of the Privacy Commissioner, Guidance Note for Departments Seeking Legislative Provision for Information Matching, 16 May 2008. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching (current version)
[6] The Privacy Commissioner, Annual Report 2010, Wellington, November 2010. http://privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-Annual-Report-2010.pdf
[7] Written by the Assistant Privacy Commissioner, Blair Stewart.
[8] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Wellington, 2002.
[9] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Auckland/Wellington, 2007 [hereafter, the NZ PIA Handbook]. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf
[10] Ibid., p. 3.

The Handbook is useful for "projects with a technological component, especially e-commerce and e-government initiatives",[11] though it also aims to help businesses, government departments and others operating offline.[12] According to the Handbook (p. 6), PIAs are an "early warning system" for agencies to enable them to detect and deal with privacy problems at an early stage so that privacy crises are averted.[13] The Handbook offers (pp. 21-28) in-depth practical advice on how to prepare privacy impact reports.

The Handbook contains 40 pages. Its contents include an overview of PIAs, an outline of the Information Privacy Principles (IPPs),[14] a discussion on PIAs (i.e., what is PIA, why it should be conducted, who should conduct PIAs, which projects require PIAs, when and how PIAs are to be conducted, guidance on PIA reports, the advantages of PIAs, and Appendices (the IPPs and a useful bibliography).

Rationale for PIAs

The Handbook outlines (p. 11) the following reasons for public and private sector agencies to conduct PIAs. First, PIAs are a "tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers". They thus function as a credible source of information. Second, a PIA enables a business to learn about the privacy pitfalls of a project (rather than its critics or competitors pointing it out to them) and helps save money and protect reputation. Third, a PIA fixes privacy responsibility with the proponent of a project – project proponents can "own" problems and devise appropriate responses. Fourth, a PIA encourages cost-effective solutions saving the expenses involved with meeting privacy concerns as a "retrofit". Fifth, a PIA leads to an initiative being privacy enhancing rather than privacy invasive. Sixth, reviews of PIA reports by the Privacy Commissioner add value to the PIA process.

The PIA process

Any agency, including medium to large businesses and government departments, that handles personal information can conduct a PIA. The Handbook prescribes (p. 13) several requirements for a person conducting PIAs (the assessor). These are:

- sound analytical and writing skills;
- familiarisation with information privacy and data protection approaches and analysis and the IPPs;
- an ability to absorb project-related paperwork and communicate with technical people;
- an ability to ask pertinent questions, understand the answers and translate them into a report that can be understood by others;
- an enquiring mind; and
- a talent for lateral thinking.

The assessor might need to draw on the skills of others and the range of necessary skills mentioned in the Handbook (p. 13) are policy development skills, operational programme and business design skills, technology and systems expertise, risk and compliance analysis skills,

[11] NZ PIA Handbook, p. 5.
[12] The Handbook cautions that it does not offer legal advice.
[13] As advocated by the Australian OVPC Guide and the UK ICO Handbook.
[14] The Information Privacy Principles are a set of 12 privacy principles based on international principles of fair information practice that agencies must comply with in the collection, accuracy, use and security of personal information. See Part 2, Section 6 of the New Zealand Privacy Act 1993.

procedural and legal skills, and information privacy and data protection expertise. Where the necessary skills to carry out a PIA exist within the organisation's project team, it may itself carry out the PIA. Otherwise, external experts with particular skills may be hired. The organisation's Privacy Officer may co-ordinate or check the PIA. If necessary, competent privacy expertise from New Zealand itself or Australia may be engaged and the assessor must work "closely alongside the project team to fully understand the business, the project, the risks and the appropriate responses" (p. 14). Where the PIA is solely an internal undertaking, the Handbook suggests incorporating external or independent oversight (p. 14).[15]

Projects with major privacy implications in more than one jurisdiction should invite comments from the privacy commissioners of those jurisdictions before finalisation of the privacy impact report. These projects must comply with the data protection and information privacy requirements in all relevant countries.

The Handbook recommends (p. 14) minimising the duplication of PIA efforts by undertaking generic or overarching PIAs where planned projects are very similar.

The Handbook cites some examples of cases when a PIA is **necessary** (p. 15): e.g., a database holding information on the entire population of New Zealand, application of new technologies to data processing and whose effects are not widely understood or trusted by the public, for systems with surveillance or intrusive capabilities and projects amassing confidential information onto accessible databases. It also cites the following cases that **might benefit** from a PIA (p. 15): merging internal business databases to enable new forms of client profiling, centralising a multi-national company's employee records in New Zealand or elsewhere and changing the manner of information collection in customer interface systems (for instance, adopting unattended kiosks, automated voice responses, smartcards and remote access tools). PIAs may also be **desirable**, according to the Handbook (p.15), in projects:

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

Wider business privacy strategies of organisations may incorporate PIAs. It is not necessary to conduct a PIA for minor changes to existing systems or programmes.

The Handbook states (p. 17) that, "Ideally, full and detailed consideration of privacy issues should precede system design." Where a PIA can only be completed later, the privacy impact report "can be an evolving document which will become more detailed over time".[16]

The Handbook says that a PIA has several phases. The first phase (prior to formal conduct of the PIA) is a *preliminary privacy analysis.* This involves documentation of the key features of the project and identification of issues without detailed study. This is useful to gauge whether

[15] The possibilities suggested are using a privacy or data protection consultant or showing the privacy impact report or a draft to the OPC.
[16] NZ PIA Handbook, p. 17.

a privacy impact report needs to be prepared, define resource requirements, suggest terms of reference for the assessment and provide a tool for initiating consultation with the Privacy Commissioner.

Following this, the organisation must choose a suitable person to prepare the report and draft the terms of reference. After this, assessment can begin. According to the Handbook (p. 19), the terms of reference "describe the project to be assessed and explain how that should be integrated into the project timeline (for example, setting deadlines for the privacy impact report which fit with key project milestones)." The terms of reference are sometimes open-ended and at other times, more focussed. They may also include a list of resource people and information on how to deal with the PIA report.

The Handbook highlights (p. 29) the advantages of PIAs: building and sustaining high levels of trust and confidence in electronic service delivery, maintaining competitive advantage, benefits to the organisation's reputation, facilitating growth by reinforcing loyalty and demonstrating the organisation's commitment to fair information practices.

The PIA report

The Handbook (p. 21) suggests the following contents (to use as a checklist) for PIA reports:

- Introduction and overview
- Description of the project and information flows
- The privacy analysis (collecting and obtaining information about use, disclosure and retention of information)
- Privacy risk assessment
- Privacy enhancing responses
- Compliance mechanisms
- Conclusions

The *Introduction and overview* (p. 21) should give an insight into an organisation's privacy management and outline its privacy policies and commitment to good standards of data protection. It might also contain information on corporate structure or outline relevant statutory authorisations or constraints (in the case of public bodies). Details such as author identities, date of the document and a glossary of special terms used should be included along with any assumptions underlying the assessment and the terms of reference.

The next part, *Description of the project and information flows* (p. 22), calls for a careful and accurate description of the project. The report must:

- provide a summary of the project including a description of the needs that led to it;
- describe the information to be used in the project;
- provide diagrams depicting the flow of personal information (i.e., flow charts must clearly depict the manner of data collection, internal circulation and dissemination beyond the organisation); and
- explain who will have access to particular categories of personal information.

The *Privacy Analysis* follows. According to the Handbook (p. 22), the privacy analysis follows the "the information 'life cycle' of collection and obtaining of personal information, through its use, retention, processing, disclosure and destruction". It must highlight the changes the project brings to previous information-handling practices, their effect on individuals and any problem areas in terms of compliance with the IPPs. The privacy analysis

must "discuss and analyse the proposal with respect to the potential advantages and risks in information privacy terms and identify best practice wherever possible."[17] The privacy analysis examines issues of information collection, use, disclosure and retention.

Collecting and obtaining information

Assessors should

- Describe the personal information collected or obtained.
- Indicate the source of each item of information.
- Describe what information will be collected directly from the individual. Explain the circumstances and means of collecting (for instance, whether information is collected as part of an existing activity or transaction or whether there will be a specific collection for the purposes of the project).
- Explain how the project complies with IPPs 1-4.[18]
- Where the information collected is part of an existing process, explain the purposes for which information is currently obtained and how these will be changed by the project.
- Where the purposes differ from the current purposes, outline how the individuals concerned will be made aware of the new purposes. Might individuals be surprised or concerned by the new purposes?
- State whether there is any sensitivity associated with the collection directly from the individual through an existing process. Will it be mandatory or voluntary?
- If information is to be collected from someone other than the individual concerned or obtained from some other database or source, explain how this is proposed to be done. Where information is to be obtained from an existing database, list the purposes for which information is held in that database and explain the extent to which the purposes of the project are compatible with those purposes.
- If information is to be obtained indirectly, explain why direct collection from the individual is not planned.
- Outline the proposed steps to make individuals aware of the project's purposes and use of the information.
- Outline what authorisation is relied upon to obtain information.
- State whether there are special sensitivities about the information to be collected (for instance, racial origins or religious affiliations, information about children) or the means of collection (for instance, the use of biometrics, fingerprinting, video or audio-recording or the tracking of a person's location).
- Check if cookies are transmitted or received if a website is involved. Is behaviour-specific information in cookies used? Is there a documented procedure concerning the type of information logged or cached about customers?
- Check whether unique identifiers will be demanded, collected or otherwise involved in the collection process?

Use, disclosure and retention of information

The Handbook describes (p. 23) information on the use, disclosure and retention of information as an "important part of any privacy impact report". The assessor should

[17] NZ PIA Handbook, p.22.

[18] These are purpose of collection of information, source of personal information, collection of information from the subject and manner of collection of personal information.

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

In the *Privacy Risk Assessment* (p. 24), the project's risks are summarised and assessed. The Handbook outlines the following risks:

- Failing to comply with either the letter or the spirit of the Act,[19] or fair information practices generally;
- Stimulating public outcry as a result of a perceived loss of privacy or a failure to meet expectations regarding the protection of personal information;
- Loss of credibility or public confidence when the public feels that a proposed project has not adequately considered or addressed privacy concerns;
- Underestimating privacy requirements with the result that systems need to be redesigned or retrofitted at considerable expense.

The Handbook reiterates (p. 24) that the expectations of the public, customers, clients or employees are an "important consideration" to acknowledge, because proposals perceived to threaten privacy often meet with public criticism and rejection.

The Handbook also highlights the following forms of privacy risks (p. 24): collection of excessive information, use of intrusive means of collection, obtaining sensitive details, unexpected or unwelcome use or disclosure of information, retention for unduly long periods, etc. The PIA report is thus a means to "identify the avoidable risks and suggest cost-effective measures to reduce them to an appropriate level". The Handbook suggests (p. 24) assessors consider the following:

- How might individuals be affected by the risks identified?
- What is the likelihood of the risks? What is the range of possible adverse outcomes from least to most severe?

[19] The Privacy Act 1993.

- Would a customer be surprised, or concerned, to see his or her details put to this use? If security were to be breached or procedures not followed, what might be the effect on individuals?
- Do the public or customers have heightened sensitivities about the data in the proposed system?
- Will the information remain in New Zealand? If data were to be transferred outside New Zealand, there are special sensitivities.

The PIA report might also include:

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

After identification of the privacy risks, there must be a suitable response. This response might be to do nothing, to abandon the project or to find middle ground. The Handbook suggests a range of *privacy enhancing responses* (p. 25) appropriate to identified risks.

The first type is *security responses.*[20] These involve incorporating appropriate security safeguards in line with the OECD proportionality principle.[21] There can also be other privacy responses (p. 26), addressing the information and management needs of the project. Does a business really need to know a particularly sensitive item of information or can it proceed without it? Similarly, are the organisation's interests best served by adding transaction data to its data warehouse or should it be erased when no longer needed? Does a particular use of information only proceed if a customer or employee opts in rather than operating on an opt-out basis? The Handbook strongly supports asking whether the business needs personal information about identifiable people to fulfill its purposes and prefers that businesses use PETs where possible.

The Handbook advises (p. 26) consideration of the following:

- Have security procedures for the collection, transmission, storage and disposal of personal information, and access, been documented?
- Are privacy controls in place for the project? These include "need to know" policies and procedures for personal information access, physical security and access controls, IT security and access controls.
- Have technological tools and system design techniques been considered which may enhance both privacy and security (e.g., encryption, technologies of anonymity or pseudonymity, PETs)?
- Has there been an expert review of all the security risks and the reasonableness of countermeasures to secure the system against unauthorised or improper collection, access, modification, use, disclosure and disposal?

[20] NZ PIA Handbook, p. 25.

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

- Have staff been trained in requirements for protecting personal information and are they aware of policies regarding breaches of security or confidentiality? Are there plans for updated training as a result of the project under review?
- Are there authorisation controls defining which staff may add, change or delete information from records?
- Is the system designed so that access and changes to data can be audited by date and user identification? Does the system "footprint" inspection of records and provide an audit trail?
- Are user accounts, access rights and security authorisations controlled and recorded by an accountable systems or records management process?
- Are access rights only provided to users who actually require access for the stated purposes of collection or consistent purposes? Is user access to personal information limited to that required to discharge the assigned functions?
- Are the security measures commensurate with the sensitivity of the information recorded?
- Are there contingency plans and mechanisms in place to identify security breaches or disclosures of personal information in error? Are there mechanisms in place to notify security breaches to relevant parties to enable them to mitigate collateral risks?
- Are there adequate ongoing resources budgeted for security upgrades with performance indicators in systems maintenance plans?
- What steps are to be taken to make affected individuals aware of the project as it affects their information? Is this to be a one-off exercise or are there ongoing implications?
- Is the privacy impact report to be made widely available? Is there to be public or stakeholder consultation, building upon the report?

Compliance mechanisms

In the section on *Compliance Mechanisms,* the Handbook (visualising systems design as a dynamic process) recommends that a PIA report outline how the organisation will address a project's privacy risks on an ongoing basis (p. 26). A PIA report completed before a project goes live is most likely to have better impact in terms of project decision-making. An interim report could precede a final report or alternately a revised report could follow a completed report. In this respect, it suggests (p. 27) that agencies consider whether:

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

The final part of the PIA report is the *Conclusion,* which is a summary conveying the following information:

- A description of the proposal including objectives, parties involved, timing and key milestones, resource requirements, benefits to the business or public, and pointers to more detailed information about the proposal.
- A list of relevant privacy requirements including applicable law, business policies and codes of practice.
- The specific privacy risks.

- Options for addressing or mitigating those risks, along with the implications of principal options examined.
- A brief analysis of experience in other organisations, in New Zealand or elsewhere, which have addressed similar risks and whether their approaches were successful.
- An identification of any residual risks that cannot be addressed through the proposed options and, where possible, the likely implications of those residual risks in terms of public reaction, project success and other business interests.
- A proposed privacy communications strategy, where appropriate, so that stakeholders are effectively informed.

The Handbook suggests (p. 27) improving readability by including Appendices with information on items such as brief discussions and summaries on aspects of data processing, tables summarising and comparing issues and documentation relevant to the PIA.

The Handbook recommends (p. 21) that the PIA report is best written with a non-technical audience in mind and that it be made publicly available (p. 19) (either in full or summary on an organisation's website).

6.3 ANALYSIS OF THE NEW ZEALAND GUIDANCE DOCUMENT

We now present a tabular analysis of the NZ PIA Handbook based upon Clarke's criteria.[22]

Clarke's criteria	NZ PIA Handbook
Status of the guidance document – obligatory, conditionally obligatory, recommended, encouraged, purely voluntary)	The use of the Handbook is encouraged. The Handbook does not offer legal advice, only provides practical guidance.
Discoverability of the guidance document in terms of PIA promotional activities for the guidance document, prominence of the document on the issuing organisation's website, number of hits, usage)	The NZ PIA Handbook features on the OPC website under *News and Publications/Guidance Notes.* It is not easily found on the Web. PIAs conducted in New Zealand have used it to guide their processes.
Applicability of the guidance document Does the document indicate a wide scope of activities to which it is applicable and clarity about geo-political area of application, clarity about categories of organisations applicable to.	The NZ PIA Handbook indicates which projects would warrant PIAs. Applicable in New Zealand. Aimed at any public or private sector agency handling personal information (particularly medium to large businesses and government departments).
Responsibility for the PIA Does it clarify that the responsibility for the conduct of a PIA rests with organisations that sponsor, propose or perform projects? Does it motivate organisational control? Does it also clarify what is and what is not a PIA?	Does not specify that the responsibility for conduct of the PIA rests with the organisations that sponsor, propose or perform projects. However, it does hold proponents of proposals responsible for privacy problems and allocates them the responsibility of devising appropriate responses. It clarifies what is and is not a PIA (it draws a distinction with privacy compliance audits).
Timing of the PIA Does it stipulate sufficiently early	Yes.

[22] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, 2011, pp. 111-120.
http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full.pdf

commencement? Does it stipulate multi-phasing where necessary?	
Scope of the PIA Has scope been clarified in terms of the dimensions of privacy, stakeholders, legal and social reference points?	Dimensions of privacy: Acknowledged in terms of "personal privacy" and personal information. Stakeholders: Several mentions of stakeholders (pp. 21, 25, 26, 27), no clarification or definition provided. The main legal reference point are the 12 IPPs in the Privacy Act 1993. Other principles, guidelines and rules of the Act might also apply. The Handbook acknowledges public expectation in protection of personal information (p. 24), public concerns in relation to inadequate consideration and addressing of privacy risks (p. 24). Calls for "achieving and maintaining public trust in electronic service delivery" (p. 3).
Stakeholder engagement – early contact with stakeholders, information provision, consultative process, early conduct of consultative process, communication of process and outcomes, exposure to draft PIA report and publication of final PIA report.	No mention of early contact with stakeholders. The Handbook mentions consultation with stakeholders (p. 26) but does not outline the consultative process. It supports empathy with "affected individuals" (p. 24). It advocates writing PIA reports with stakeholders in mind (p. 21). It suggests making completed PIA reports publicly available (e.g., posting the report or a summary on website).
Orientation – Process cf. product; solutions cf. problems	A PIA is envisaged as a "systematic process". The approach, here, appears more solution-oriented.
The PIA process Does it describe the preliminary privacy issues analysis process? Does it outline phases or structure? Does it provide sufficient detail about activities within each phase? Does it lead an organisation to move the outcomes forward through the design and implementation phases? Does it give guidance on the contents of a PIA report?	The Handbook describes the preliminary privacy issues analysis process. It focuses less on phases of a PIA and more detailed focus on preparing a PIA report.
Role of the oversight agency (i.e., the New Zealand OPC)	The agency conducting the PIA may consult the Privacy Commissioner in the preliminary privacy analysis phase (p. 17). It may review the PIA report (or draft) (p. 11). It may receive the PIA report for information only or offer feedback and constructive suggestions (p. 14).

6.4 LEGAL BASIS

1. General framework for privacy and data protection

New Zealand does not have a written constitution, i.e., there is no single supreme document. The New Zealand Bill of Rights Act 1990[23] and the Human Rights Act 1993[24] are the basic instruments for fundamental rights protection in New Zealand. Art. 21 of the Bill of Rights provides for protection against unreasonable search or seizure. The New Zealand Court of Appeal has interpreted this provision in several cases as protecting the right to privacy.[25]

The general privacy and data protection instrument in New Zealand is the **Privacy Act 1993**.[26] The Act created the Privacy Commissioner.[27]

The **Health Information Privacy Code 1994**,[28] issued pursuant to sections 46-53 of the Privacy Act 1993, has the effect of law on all health agencies that are holding, using or disclosing health information.

2. Laws on PIA forerunners

Section 13 of the Privacy Act 1993 provides for a form of **prior consultation** that applies also for data matching (information matching):[29]

> (1) The functions of the Commissioner shall be –
> (f) to examine any proposed legislation that makes provision for –
> (i) the collection of personal information by any public sector agency; or
> (ii) the disclosure of personal information by one public sector agency to any other public sector agency –
> or both; to have particular regard, in the course of that examination, to the matters set out in section 98 [Information matching guidelines], in any case where the Commissioner considers that the information might be used for the purposes of an information matching programme; and to report to the responsible Minister the results of that examination.

3. PIA legal bases

Section 32 of the **Immigration Act 2009**[30] explicitly requires PIA be conducted if biometric information are processed:

---

[23] New Zealand Bill of Rights Act 1990, Public Act 1990 No 109.
http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html
[24] Human Rights Act 1993, Public Act 1993 No 82.
http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html
[25] Privacy International, *Privacy and Human Rights 2006. Country Reports – New Zealand*, 2007.
https://www.privacyinternational.org/article/phr2006-new-zealand. Art. 29 Working Party, *Opinion 11/2011 on the level of protection of personal data in New Zealand*, WP 182, adopted on 4 April 2011.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf
[26] Privacy Act 1993, Public Act 1993 No 28.
http://www.legislation.govt.nz/act/public/1993/0028/latest/096be8ed80744ad4.pdf (official source).
[27] Office of the Privacy Commissioner. http://privacy.org.nz
[28] Health Information Privacy Code 1994. http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary.pdf.
[29] Part 10 and Schedule 4 of the Privacy Act govern information matching. The Privacy Commissioner has a regulatory role to control the use of data matching by government departments. The Parliament can pass legislation to permit departments to share information through authorised information matching programmes. All data matching programmes have their legislative provision included in Schedule 3 of the Privacy Act. Cf. http://privacy.org.nz/data-matching-introduction

(1) The Department must complete a privacy impact assessment in respect of the collection and handling of biometric information under this Act to –
(a) identify the potential effects that the Act may have on personal privacy; and
(b) examine how any detrimental effects on privacy might be lessened.

(2) The Department must consult the Privacy Commissioner –
(a) on the terms of reference developed for the assessment; and
(b) when completing the assessment.

(3) The Department must review its privacy impact assessment if changes are made to this Act, regulations made under it, or operational policy in respect of the collection or handling of biometric information and, if the review establishes that new or increased privacy impacts have resulted from the changes, must –
(a) amend or replace the privacy impact assessment; and
(b) consult the Privacy Commissioner on the amended or replacement assessment.

(4) The Department must ensure the current privacy impact assessment is –
(a) available on the Department's Internet site; and
(b) available or readily obtainable for inspection, free of charge, at –
(i) offices of the Department; and
(ii) New Zealand government offices overseas that deal with immigration matters.

(5) Nothing in subsection (4) requires the making available of information that could properly be withheld in accordance with the provisions of the Official Information Act 1982, were a request to be made for the information under that Act.

4. Guidance material

In July 2008, the Office of the Privacy Commissioner has issued a PIA handbook[31] and a guidance note on information matching PIA.[32]

6.5 COMMENTS ON THE SHORTCOMINGS AND EFFICACY OF PIA IN NEW ZEALAND BY PIA EXPERTS

Roger Clarke has commented that the NZ PIA Handbook is "of moderate to good quality, but with material shortfalls".[33] He substantiates this based on the long-standing existence of the Handbook and the intellectual expertise of Assistant Privacy Commissioner Blair Stewart, one of the leaders of the PIA movement. According to Clarke, the Handbook's weaknesses are a strong emphasis on legal compliance, the limited mention of broader concerns and public expectations, and little impetus for public engagement. Clarke further states, "Relatively few

[30] Immigration Act 2009, Public Act 2009 No 51.
http://www.legislation.govt.nz/act/public/2009/0051/latest/096be8ed806837b3.pdf
[31] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook.*
http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf
[32] Office of the Privacy Commissioner, *Guidance Note for Departments Seeking Legislative Provision for Information Matching: Information Matching Privacy Impact Assessments*.http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching
[33] Clarke, op. cit., 2011.

PIAs have been conducted, but a number have for large government projects".[34] He adds, "Although a preference for openness about the findings is expressed, only a couple of PIA Reports have been published."[35]

Blair Stewart, one of the pioneers in developing and stimulating the adoption of the PIA concept in the mid-1990s,[36] and author of the New Zealand Handbook, details his experience of PIAs.[37] According to him, PIAs are:

- being hurriedly undertaken for a major public initiative just weeks out from the critical decision being taken and while omitting a detailed study phase;
- driven by an agency committed to a particular option with the resultant report slanting coverage of the issues and including a number of unsubstantiated assertions in favour of the proposal;
- focusing almost exclusively on legal issues without specialist analysis of important technical risks;
- attempted by a part-time committee without the time to bring its work to a conclusion while, in tandem, decisions on the project were being taken in reliance upon incomplete versions of the PIA documentation.

John Edwards provides a law practitioner's perspective of PIAs in New Zealand.[38] Edwards observes that prior to the New Zealand PIA Handbook,

> Early efforts at objective and methodical evaluation of privacy impacts produced varied results. Some were little more than sales pitches, with benefits hyperbolically overstated, projections hopelessly optimistic, and negatives glossed over, barely touched, or simply dismissed as small, private and insignificant incidents of the greater public good that would be served.[39]

According to Edwards, the Handbook formalised, institutionalised and brought PIAs into the mainstream of New Zealand. PIAs are now "commonplace, being commissioned and prepared in respect of a wide range of innovations and proposals".[40]

On the negative side, Edwards comments that there are "different assumptions among clients, regulators and others as to what the assessment process is intended to do and is capable of delivering". Assessments based primarily on compliance are not "going to be a comprehensive review of privacy issues". Assessments, he states, pose "definitional challenges" even if their scope is limited to data flows. He further notes,

---

[34] Ibid.

[35] Citing Information Commissioner's Office, *Privacy Impact Assessments: International Study of their Application and Effects*, Appendix F - Privacy Impact Assessments: Jurisdictional Report for New Zealand, ICO, Wilmslow, UK, December 2007.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_appf_nz_2910071.pdf

[36] See Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review*, Vol. 25, No. 2, April 2009, pp. 123-135; Tancock, David, Siani Pearson and Andrew Charlesworth, *The Emergence of Privacy Impact Assessments*, HP Labs Technical Report (HPL-2010-63), 2010. http://www.hpl.hp.com/techreports/2010/HPL-2010-63.html

[37] Stewart, Blair, "Privacy Impact Assessment: Towards a Better Informed Process for Evaluating Privacy Issues Arising from New Technologies", *Privacy Law & Policy Reporter*, Vol. 5, No. 8, 1999, pp. 147-149.
http://www.austlii.edu.au/au/journals/PLPR/1999/#no8]

[38] Edwards, John, "Privacy Impact Assessment in New Zealand – A Practitioners' Perspective," in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

[39] Ibid.

[40] Ibid.

> If disregarding a "compliance based" approach makes sense in order to ensure the issues are widely canvassed, it presents another challenge, that of subjectivity. "Complies with"/"does not comply with" reports are crude, but at least have the virtue of objectivity. The activity is being measured against the standard set in law.[41]

6.6 BEST ELEMENTS

Among the elements of PIA in New Zealand that we most like are the following:

- PIAs are regarded as "systematic processes".
- PIAs are regarded as "early warning systems".
- A distinction is drawn between PIAs and privacy compliance audits.
- The Handbook says that the proponent of a proposal is responsible for privacy. The proponent must "own" problems and devise appropriate responses in the design and planning phases.
- It provides for review of privacy impact reports by the Privacy Commissioner.
- It lists the variety of skills required for undertaking an assessment and completing a privacy impact report, thus highlighting the importance of employing people with the right competencies to conduct PIAs.
- It provides that PIAs must invite comments from privacy commissioners of all jurisdictions where projects are likely to have significant privacy implications and to ensure that PIAs in such projects meets or exceeds the data protection and information privacy requirements in all the relevant countries.
- It has a useful bibliography of national and international PIA resources.
- While it does not go into much detail, it does envisage consultation with stakeholders.
- It favours publication of PIA reports or, at least, summaries.

[41] Ibid.

7 UNITED KINGDOM

7.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

The Information Commissioner's Office (ICO) is credited with launching privacy impact assessment in the UK. In 2007, the ICO commissioned a team of experts co-ordinated by Loughborough University to study PIAs in other jurisdictions (Australia, Canada, Hong Kong, New Zealand and the United States) and identify lessons to guide PIAs in the UK.[1] In 2007, the ICO published a PIA handbook[2] and became the first country in Europe to do so.

The Handbook, revised in 2009,[3] forms a crucial basis of the PIA process. According to the ICO, a PIA is "a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions."

The Data Sharing Review Report reiterated the need for PIAs and recommended their use.[4] The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start".[5] It accepted the value of PIA reports and stressed that they will be used and monitored in all departments (as a means of protecting personal data and tackling identity management challenges from July 2008 onwards).[6] PIAs have thus become a "mandatory minimum measure".[7]

According to the ICO Annual Report of July 2010, "over 300 Privacy Impact Assessments have been started across central government and their agencies".[8]

---

[1] ICO, *Privacy Impact Assessments: International Study of their Application and Effects*, Information Commissioner's Office, Wilmslow, Cheshire, UK, December 2007.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf

[2] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 1.0, December 2007.

[3] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009 (hereafter ICO Handbook 2009)
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html,
http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

[4] Thomas, Richard, and Mark Walport, *Data Sharing Review Report*, 11 July 2008.
http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf; incorporated into CESG (the UK Government's National Technical Authority for Information Assurance), *HMG Information Assurance Standard No 6 – Protecting Personal Data and Managing Information Risk*. http://www.cesg.gsi.gov.uk/ia-policy-portfolio/hmg-ia-standards.shtml

[5] Cabinet Office, Data Handling Procedures in Government: Final Report, June 2008, p. 18.
http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf

[6] These are expected to become an integral part of the risk management assessment and will be checked by future "Gateway™" reviews of ICT projects. Gateway reviews are undertaken by an independent team of experienced people and carried out at key decision points in government programmes and projects to provide assurance that they can progress successfully to the next stage.

[7] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews". http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

[8] ICO, Information Commissioner's Annual Report 2009/10: Upholding Information Rights in a Changing Environment, HC 220, The Stationery Office, London, 13 July 2010, p. 23.
http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf

7.2 THE ICO PRIVACY IMPACT ASSESSMENT HANDBOOK (VERSION 2)

The ICO Handbook (Version 2) is 86 pages long and is available on the ICO website, under its section on data protection.[9] Its contents include: background information (PIA and other processes, rationale for PIAs, end results of effective PIAs, management of PIAs, conduct of PIAs, privacy, risks and solutions), the PIA process, the PIA screening questions, data protection compliance checklist template, Privacy and Electronic Communications Regulations (PECR) compliance checklist and privacy strategies.

This section outlines the PIA framework as embodied in the Handbook.

The ICO envisages a PIA as a process, separate from "compliance checking or data protection audit processes",[10] that should be undertaken when it can "genuinely affect the development of a project".[11] The Handbook distinguishes a PIA from a privacy or data protection audit. An audit is conducted post implementation of a project, a PIA prior to it. An audit confirms compliance privacy undertakings and/or privacy law and highlights problems that need addressing while a PIA intends to prevent problems.

According to the Handbook, a PIA is necessary for the following reasons: To identify and manage risks (signifying good governance and good business practice); to avoid unnecessary costs through privacy sensitivity; to avoid inadequate solutions to privacy risks; to avoid loss of trust and reputation; to inform the organisation's communication strategy and to meet or exceed legal requirements. Additionally, the Handbook highlights the results of an effective PIA:[12]

- The identification of the project's privacy impacts;
- An appreciation of those impacts from the perspectives of all stakeholders;
- An understanding of the acceptability of the project and its features by the organisations and people who will be affected by it;
- The identification and assessment of less privacy-invasive alternatives;
- An identification of ways in which negative impacts on privacy can be avoided;
- An identification of ways to lessen negative impacts on privacy;
- Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- Documentation and publication of the outcomes.

The Handbook says that PIA should be conducted early in the project development so that risks and problems can be identified and managed efficiently. For projects already in existence, the Handbook says that the time to act is the present. The ICO conceives of a PIA as a "cyclical process linked to the project's own life-cycle; and re-visited in each new project phase".[13]

Management of the PIA

[9] ICO, Privacy Impact Assessment. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx
[10] ICO Handbook 2009, Part I, Chapter I.
[11] Ibid. The Handbook uses the term "project" as a catchall; it can refer to "a system, database, program, application, service or a scheme, or an enhancement to any of the above, or an initiative, proposal or a review, or even draft legislation".
[12] Ibid.
[13] ICO Handbook, Part I, Chapter I.

The Handbook places responsibility for managing a PIA at the senior executive level (preferably someone with lead responsibility for risk management, audit or compliance) with the following objectives in mind:

- Ensuring effective management of the privacy impacts arising from the project;
- Ensuring effective management of the risks arising from the project's privacy impacts; and
- Avoiding expensive re-work and retrofitting of features, by discovering issues early, devising solutions at an early stage in the project life-cycle, and ensuring that they are implemented.

In the case of delegation of the responsibility of carrying out a PIA, the Handbook recommends it take the form of either an appointment within the overall project team, someone outside the project or an external consultant.[14] Irrespective of who conducts the PIA, the direct responsibility for the PIA rests with the organisation. A project steering committee (with directive powers), or a project advisory committee or project reference or consultative group (to discuss, advise and assist, but with no formal powers to direct the process) may be established to assist in the PIA process. If the PIA is delegated to an organisation's data protection or privacy officer, the ICO recommends that the officer is made part of the steering committee or consultative group. Responsibility should only be delegated to an officer who has "sufficient authority to influence the design and development of a project and participate fully in the project design decisions".

Furthermore, the Handbook advises that the terms of reference for the PIA be prepared and agreed.[15] These should include the following:[16]

- the functions to be performed;
- the deliverables;
- the desired outcomes;
- the scope of the assessment; and
- the roles and responsibilities of various parties involved in the PIA.

Role of the Information Commissioner

The ICO does not play a formal role in conducting, approving or signing off PIA reports. It does, however, play an informative and consultative role in supporting organisations in the conduct of PIAs.

The PIA process

The ICO recommends the following set of phases for a PIA: preliminary, preparation, consultation and analysis, documentation and review and audit. These phases occur in both full-scale and small-scale PIAs, though they differ in scope.[17]

1. Preliminary

[14] The Handbook cautions that "the advantages of employing an independent consultant need to be weighed against the disadvantages of resistance to the conclusions reached during the PIA, the potential lack of understanding or appreciation of the organisation's needs and the business case for the project".
[15] The Handbook does not specify by whom this is to be done.
[16] ICO Handbook, Part I, Chapter I.
[17] Phases or tasks may be compressed or consolidated in the case of small-scale PIAs.

This phase focuses on establishing a firm basis for the "effective and efficient" conduct of the PIA. The Handbook suggests two deliverables for this phase – a project plan and a project background paper. Tasks suggested for this phase include: reviewing outcomes and documents from the initial assessment; developing the project outline;[18] ensuring appropriateness of terms of reference, scope and PIA resources; preliminary discussions with relevant organisations and stakeholder groups; preliminary analysis of privacy issues; and preparation of the project background paper.

2. Preparation

In this stage, arrangements are made in anticipation of the critical consultation and analysis phase. The ICO Handbook suggests the following deliverables for this stage: a stakeholder analysis, a consultation strategy and plan, and establishment of a PIA consultative group (PCG).

3. Consultation and analysis

Here, consultations with stakeholders, risk analysis, problem recognition and solution search are envisaged.

4. Documentation

This phase focuses on documenting the PIA process and its results (primarily in the form of a PIA report).

5. Review and audit

This phase confirms that the results of the PIA are implemented by the organisation and are effective.

The Handbook also outlines an **overview of the PIA process**.

Initial assessment: This is an examination of a project at an early stage with a view to initially determining privacy risks and what further assessment might be necessary. Here, preparations are made, a stakeholder analysis is carried out, information is gathered, privacy risks are determined and finally an assessment is made as to what level of PIA is required.

Full-scale PIA: This is a more comprehensive internal privacy risk assessment in cases where there is a chance of a substantial privacy impact. A full-scale PIA encompasses privacy risk analysis, stakeholder consultation and proposal of solutions to the risks. The criteria for determining if a full-scale PIA is required are set out in Appendix 1, Step 1 of the Handbook. The criteria are set out as questions, the answers to which, when considered as a whole, would indicate whether a full-scale PIA is warranted. The questions are:[19]

1. Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?
2. Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

[18] A list of contents is provided in the ICO Handbook.
[19] ICO Handbook, Appendix A, Step 1.

3. Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?
4. Does the project involve multiple organisations, whether they are government agencies (e.g., in "joined-up government" initiatives) or private sector organisations (e.g., as outsourced service providers or as "business partners")?
5. Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?
6. Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?
7. Does the project involve new or significantly changed handling of personal data about a large number of individuals?
8. Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?
9. Does the project relate to data processing which is in anyway exempt from legislative privacy protections?
10. Does the project's justification include significant contributions to public security measures?
11. Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

Examples of some full-scale PIAs are the PIA for the 2011 Census for Northern Ireland,[20] PIA for the 2011 Census for England and Wales[21] and the PIA on the IMPACT Programme (the Police National Database).[22]

Small-scale PIA: This is a less formal version of a full-scale PIA, involving less investment and fewer resources, less exhaustive analysis and information gathering and generally used to study specific project aspects. The Handbook cites instances[23] where a small-scale PIA might be appropriate: Replacement of an existing personal data system by new packaged software; plans to outsource business processes involving personal data, or the storage and processing of personal data; application of existing personal data to a new purpose; or changes to retention policies relating to personal data. The Handbook sets out a list of 15 criteria for evaluating whether a small-scale PIA is required:[24]

1. Does the project involve new or inherently privacy-invasive technologies?
2. Is the justification for the new data-handling unclear or unpublished?
3. Does the project involve an additional use of an existing identifier?
4. Does the project involve use of a new identifier for multiple purposes?
5. Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

[20] Northern Ireland Statistics and Research Agency, Report of a Privacy Impact Assessment Conducted by the Northern Ireland Statistics and Research Agency in relation to the 2011 Census Northern Ireland, May 2010. http://www.nisranew.nisra.gov.uk/census/pdf/Privacy%20Impact%20Assessment.pdf

[21] Office for National Statistics, Report of a Privacy Impact Assessment Conducted by the Office for National Statistics in relation to the 2011 Census England and Wales, November 2009. http://www.ons.gov.uk/census/2011-census/2011-censusproject/commitment-to-confidentiality/privacy-impact-assessment--pia--on-2011-census.pdf

[22] National Policing Improvement Agency (NPIA), IMPACT Programme: Police National Database Privacy Impact Assessment Report, April 2009. http://www.npia.police.uk/en/docs/Privacy_Impact_Assessment.pdf

[23] See full listing in the ICO Handbook.

[24] ICO Handbook, Appendix 1, Step 2.

6. Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?
7. Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?
8. Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?
9. Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?
10. Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?
11. Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?
12. Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?
13. Does the project involve new or changed data retention arrangements that may be unclear or extensive?
14. Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?
15. Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?

If answers to the questions are positive, the extent of privacy impact and consequent project risk is considered. If only one or two aspects raise privacy concerns, a small-scale PIA addressing those concerns is justified. If the answers to multiple questions are positive, a full-scale PIA is required. Examples of small-scale PIAs are PIA on the exchange of fingerprint information with immigration authorities in Australia, Canada, New Zealand and the United States[25] and the PIA by UK Anti-Doping in relation to personal information disclosed to it by the Serious Organised Crime Agency.[26]

Privacy law compliance check: This check determines whether there is compliance with privacy and data protection laws such as the Human Rights Act 1998, the ***Regulation of Investigatory Powers Act*** 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Data Protection Act 1998.

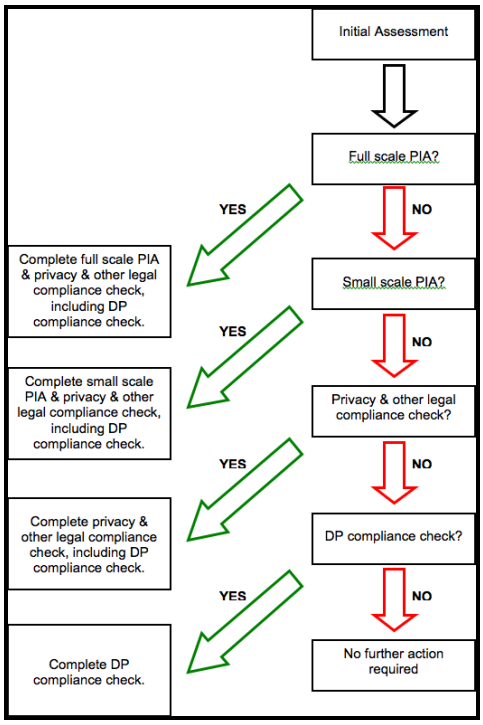
Data protection compliance checklist: This is generally carried out after implementation of the project and is a checklist for compliance with the Data Protection Act 1998.

Review and re-do: This stage envisages a timetable for reviewing actions taken after the PIA and their effectiveness. It also envisages checking whether new aspects of projects might be subject to a PIA.

The Handbook envisages the process as depicted below:

[25] Home Office UK Border Agency, Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the Immigration authorities of the Five Country Conference, 2009.
http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/pia.pdf?view=Binary

[26] UK Anti-Doping, Report of a Privacy Impact Assessment conducted by UK Anti-Doping in relation to Personal Information disclosed to it by the Serious Organised Crime Agency, 15 January 2010.
http://www.ukad.org.uk/docLib/Reports/PIA_report_150110.pdf



The PIA report

A key deliverable of the documentation phase is the PIA report. The ICO Handbook sets out the following reasons for preparing a PIA report:

- as an element of accountability, in order to demonstrate that the PIA process was performed appropriately;
- to provide a basis for post-implementation review;
- to provide a basis for audit;
- to provide corporate memory, ensuring that the experience gained during the project is available to those completing new PIAs if original staff have left; and,
- to enable the experience gained during the project to be shared with future PIA teams and others outside the organisation.

It also sets out the key elements of a PIA report:

- A description of the project;
- An analysis of the privacy issues arising from it;
- The business case justifying privacy intrusion and its implications;
- Discussion of alternatives considered and the rationale for the decisions made;
- A description of the privacy design features adopted to reduce and avoid privacy intrusion and their implications of these design features;
- An analysis of the public acceptability of the scheme and its applications.

The ICO Handbook lists the following sources for content of the PIA:

- A summary of the consultative processes undertaken;
- Contact details of organisations and individuals with whom consultations were undertaken;
- The project background paper(s) provided to those consulted;

- The PIA project plan;
- The issues register and/ or privacy design features paper(s);
- References to relevant laws, codes and guidelines.

The appendices of a PIA report could include a privacy law compliance study and a data protection compliance study, after legal compliance checks are complete. A PIA report needs to be complete, informative and comprehensible.

When a PIA report is published or widely distributed, it can fulfil the functions listed above (i.e., accountability, post-implementation review, audit, provide corporate memory and enable experience sharing). However, if information collected during the PIA process is commercially or security sensitive, it could be redacted or placed in confidential appendices, if justifiable.

7.3 MINISTRY OF JUSTICE PIA GUIDANCE (2010)

The UK Ministry of Justice produced its own PIA guidance (hereinafter MOJ Guidance) in August 2010.[27] It aims to provide guidance for government officials on how to conduct PIAs as it contends that the ICO Handbook insufficiently provides this.[28] According to this 21-page guidance, a PIA's function is "to ensure that data protection risks are properly identified and addressed wherever possible, and that decision-makers have been fully informed of the risks and the options available for mitigating them", and not "to dictate specific courses of action, or to curtail the range of options in terms of program design or technology".[29] The MOJ views a PIA as a tool that enhances the public's understanding of Government's management of data protection issues and consequently increases public trust and confidence. PIAs are also envisaged as living documents that "develop over time"[30] – as the policy or project develops. The MOJ Guidance advocates that "PIAs should be incorporated into existing procedures for developing new policies or initiatives that involve the processing of personal data."[31]

When a PIA is required and what needs addressing in a PIA

The MOJ Guidance sets out two key criteria to determine if a PIA is required. The first is whether the proposal will involve the processing of personal data of individuals. The second is whether a PIA has already been conducted. If the proposal will involve the processing of personal data and there is no existing PIA, then the Guidance recommends that an initial screening process[32] be undertaken to identify risks and issues and how detailed a PIA is warranted.

According to the MOJ Guidance, the PIA must address the eight protection principles or principles of good information handling enshrined in Part 1 of Schedule 1 of the Data

[27] Ministry of Justice, Undertaking Privacy Impact Assessments: The Data Protection Act 1998, Ministry of Justice, 13 August 2010. http://www.justice.gov.uk/guidance/docs/pia-guidance-08-10.pdf
[28] See p. 4, which states that the ICO's handbook is "particularly useful for non-Governmental bodies in ensuring that an initiative is compliant with a wide range of legislation, including the Human Rights Act 1998".
[29] MOJ Guidance, p. 4.
[30] MOJ Guidance, p. 4.
[31] MOJ Guidance, p. 2.
[32] Outlined in MOJ Guidance, Part 4, p. 7.

Protection Act 1998.[33] These are: fair and lawful processing of data, processing for specific and lawful purposes, adequacy and relevance of data, data accuracy, limited data retention, processing in accordance with the data subject's rights, data security and restriction on personal data transfer outside the European Economic Area (EEA).

The screening process

The MOJ Guidance provides screening questions (adapted from the ICO's Handbook to focus on data protection) to determine whether a full-scale or small-scale assessment is required.

Criteria for a full-scale PIA

The MOJ Guidance sets out the following 11 questions:[34]

Technology:
Does the proposal apply new or additional information technologies that could affect an individual such as locator technologies (including mobile phone location)?

Identity:
Does the proposal involve new identifiers or re-use of existing identifiers, such as digital signatures?
Might the proposal have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

Multiple organisations:
Does the proposal involve multiple organisations, whether they are Government agencies (for example, in "joined-up Government" initiatives) or private sector organisations (for example, as outsourced service providers or as "business partners")?

Data:
Does the proposal involve new or significantly different handling of personal data that may be of particular concern to individuals?
Does the proposal involve new or significantly different handling of a considerable amount of personal data about each individual in the database?
Does the proposal involve new or significantly different handling of personal data about a large number of individuals?
Does the proposal involve new or significantly different consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

Exemptions:
Does the proposal relate to data processing which is in any way exempt from legislative data protection measures, for example, processing of personal data for the purposes of national security?

[33] The principles mirror those in the EU Data Protection Directive. European Parliament and the Council, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.
http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[34] MOJ Guidance, Part 4, Step 1, p. 7.

Does the proposal's justification include significant contributions to public security measures, for example, serious convicted offenders who have served their sentence and are released into the community. In these cases, personal data may need to be shared to ensure the safety of the public.

Does the proposal involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable data protection regulation?

The Guidance cites two examples of where a full-scale PIA might be needed: first, the establishment of a new ICT system processing a large amount of personal data (including sensitive personal data), and second, publication of a register containing personal data.[35]

Criteria for small-scale PIA

The MOJ Guidance sets out the following questions for determining if a small-scale PIA is required:[36]

Technology:
Does the proposal involve new technologies or technologies that can substantially reveal personal information, such as visual surveillance, digital image and video recording?

Justification:
Is the justification for the new data-handling unclear or unpublished?

Identity:
Does the proposal involve an additional use of an existing identifier?

Does the proposal involve use of a new identifier for multiple purposes?

Does the proposal involve new or substantially changed identity authentication requirements that may seek excessive personal information or be onerous upon an individual? It is important that identity authentication is proportionate to the purpose. For example, in some situations, face-to-face contact may have a lower threshold for identity authentication while electronic transactions may have a higher threshold of authentication and may seek more than one assurance.

Data:
Will the proposal result in the handling of a significant amount of new personal data about each person, or significant change in existing data-holdings?

Will the proposal result in the handling of new personal data about a significant number of people or a significant change in the population coverage?

Does the proposal involve new linkage of personal data with data in other collections, or significant change in data linkages?

Data handling:

[35] MOJ Guidance, p. 8.
[36] MOJ Guidance, Part 4, Step 2, p. 7.

Does the proposal involve new or different data collection policies or practices that may be unclear or seek excessive information that is not relevant to the purpose? Data controllers should seek to identify the minimum amount of information that is required in order to properly fulfil their purpose. Processing excessive amounts of information that is not required for the purposes of the data controller will be in breach of the data protection principles.

Does the proposal involve new or different data quality assurance processes and standards that may be unclear or unsatisfactory?

Does the proposal involve new or different data security arrangements that may be unclear or unsatisfactory?

Does the proposal involve new or different data access or disclosure arrangements that may be unclear or permissive?

Does the proposal involve new or different data retention arrangements that may be unclear or extensive?

Does the proposal involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

Exceptions:

Will the proposal give rise to new or changed data-handling that is in any way exempt from legislative data protection measures? This could include, for example, national security information systems.

The Guidance cites examples of where small-scale PIAs are applicable: new software installation and changes to personal data retention policies.

Even if the criteria for a full-scale or small-scale PIA are not met, a check for conformity with the Data Protection Act 1998 must still be carried out.

Phases of a PIA

The MOJ Guidance outlines the following phases in the PIA process: background phase, consulting, considering options, producing the PIA report and tying up loose ends.

1. Getting started – background phase

This is the preparatory or introductory phase. The scope of this phase involves the provision of a detailed description of the "essential aspects of the data processing elements of the proposal and identifying significant potential risks", which could include the following:[37]

- A description of the context or setting in which the proposal is being brought forward;
- A description of the personal data to be used;
- A description of the proposal's design including data flow process;

[37] MOJ Guidance, p. 12.

- Any media activity surrounding the proposal;
- An initial assessment of potential data protection issues and risks of the data sharing/data processing proposal;
- Impact upon individuals and their right to have their personal data protected;
- The justification for the features that give rise to significant impact upon individuals.

According to the MOJ Guidance (p. 12), this part should "contain a clear and well-argued case for the project as a whole, and particularly for those features that have greatest potential for significant negative impacts on data subjects". This is with the intent of identifying and examining the risks of the proposal.

2. Consulting

The next phase is the consultation with stakeholders. Interested parties (including external)[38] must have the opportunity to express their views. Organisations must find possible solutions for any identified risks. The Ministry recommends giving thought to the choice of interested parties (a wide range of stakeholders[39] is important), their influence (and impact) and the consultation method. The MOJ Guidance recommends an earlier consultation (p. 13) to "reduce resistance to the eventual solution and lead to a more comprehensive PIA". The process includes the formation of a PIA consultative (or similar) group to provide feedback and the development of a communication process to enable effective interchange of ideas (e.g., workshops, meetings).

3. Considering options

The third phase of the process aims to ensure that the project manager or assessor identifies any data protection risks of the proposal early on and finds effective solutions, where possible. In preparing a consultation, the project managers must ensure maximum representation of relevant perspectives and gather appropriate information to feed into the design and implementation of the proposal. This phase covers the following:

- Identification of design issues and any data protection concerns by the PIA consultative group and/or other interested parties;
- Working with stakeholders to redesign the process to minimise concerns;
- Recording data protection issues identified, avoidance and reduction measures considered and either rejected or adopted, design changes to be undertaken as a result, and outstanding issues;
- Incorporating decisions on design features and, where there are unresolved issues, continuing consultation and analysis; and
- Ensuring that the minimum data security requirements (recommendations of the Data Handling Review) are met.

This phase can be an ongoing, repetitive one – depending on the proposal and the nature of the issues raised.

4. Producing the PIA report

[38] Considered important for an "outside perspective".

[39] As examples, the Guidance suggests (p. 13) pressure/civil liberty groups, other government departments, regulatory bodies, third sector bodies, legal specialists and specific representative groups.

The MOJ recommends that the PIA process be documented. According to the MOJ Guidance (p.14), the final PIA report should contain:

- A description of the proposal, including the data flows;
- The case justifying the need to process an individual's personal data and why the particular policy or project is important;
- An analysis of the data protection issues arising from the policy or project;
- Details of the parties involved in the development;[40]
- Details of the issues and concerns raised, including those identified as a result of a consultation;
- Discussion of any alternatives considered to meet those concerns, and the rationale for the decisions made;
- A description of the design features adopted to reduce accessibility of an individual's personal data and the implications of these design features (where necessary), including safeguards incorporated;
- An analysis of the public acceptability of the scheme and its applications;
- Compliance with the DPA's eight data protection principles;[41]
- Compliance with the Data Handling Review's security recommendations.[42]

The Guidance (p.14), recalling the exhortation of the Data Handling Review, calls for periodic reports to be published or distributed,[43] where required, to maintain the transparency of data sharing initiatives, either on a step-by-step basis on completion of key milestones or post final assessment. The Guidance favours a full disclosure of the PIA report (publication in full) unless an exemption in the Freedom of Information Act 2000 (FOIA)[44] is warranted.[45]

5. Tying up loose ends

The PIA process concludes with the implementation of the conclusions of the PIA report into the relevant proposal or project. This might require a revisitation of the PIA report to ensure correct implementation by the relevant implementation team within each government department.

7.4 ANALYSIS OF THE TWO UK GUIDANCE DOCUMENTS

The following is a tabular analysis of the two UK PIA guidance documents based upon Clarke's criteria.[46]

Clarke's criteria	ICO PIA Handbook 2009	MOJ Guidance 2010

[40] The MOJ Guidance does not specify whether this refers to development of the project or the PIA.
[41] The Data Protection Act 1998.
[42] See Cabinet Office, Data Handling Procedures in Government: Final Report, Annex V, June 2008. http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf
[43] Neither the MOJ Guidance nor the Data Handling Review specify by whom this is to be done.
[44] See Part II of the Freedom of Information Act 2000.
[45] Where such exemptions are engaged, the public interest test must be carried out to determine disclosure. For details on the public interest test, see: ICO, Freedom of Information Act, Environmental Information Regulations: The Public Interest Test, Version 3, 3 July 2009. http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/fep038_public_interest_test_v3.pdf
[46] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, 2011, pp. 111-120. http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full.pdf

Status of the guidance document – obligatory, conditionally obligatory, recommended, encouraged, purely voluntary	Purely guidance; use is encouraged for corporations and government; recommendatory; voluntary; self-assessment tool	Informative; to help government officials undertake PIAs when ICT systems processing personal data are introduced [to be taken as a high level starting point; recommended but voluntary]
Discoverability of the guidance document – in terms of PIA promotional activities for the guidance document, prominence of the document on the issuing organisation's website, number of hits, usage	It is the top result in a Google search for the term. Accessible on the ICO website under section on Data Protection but not easily accessible unless one knows where to find it.	Can be accessed on the MOJ website under Annex D of the Data Sharing Protocol.
Applicability of the guidance document Does the document indicate a wide scope of activities to which it is applicable and clarity about geo-political area of application, clarity about categories of organisations applicable to	Scope outlined in terms of privacy risks, impacts and vulnerabilities in projects. Applicable in the UK (geo-political scope not mentioned in the Handbook). Aimed at corporations and government.	PIAs are aimed at "proposed workstreams or amendments to existing workstreams that involve the processing of personal data".[47] Applicable in the UK (no mention of geo-political scope). Applicable to government only in evaluating systems that process personal data
Responsibility for the PIA Does it clarify that the responsibility for the conduct of a PIA rests with organisations that sponsor, propose or perform projects? Does it motivate organisational control? Does it also clarify what is and what is not a PIA?	Responsibility clearly outlined in broad and specific terms. Broadly, the organisation is directly responsible. Calls for vesting responsibility for a PIA with a senior executive. Motivates organisational control. It clarifies what is and is not a PIA (draws distinction between PIA and data protection or privacy audit.)	No defined responsibility allocated. Advises that it is appropriate for someone with a detailed knowledge of that (department or team's) policy to "have responsibility for the PIA process".[48] No motivation of organisational control. No direct clarification on what is or is not a PIA; rather only outlines objectives and scope of PIA.
Timing of the PIA Does it stipulate sufficiently early commencement? Does it stipulate multi-phasing where necessary?	Recommends early commencement [Part I, Ch 1; Part II, Ch IV, 3].	Early commencement not stressed; only suggested in concluding part (Part 8, useful tips). Begins with ICO definition of PIA, so early commencement could be stipulated; PIA process envisaged as "living" document.[49]
Scope of the PIA Has scope been clarified in terms of the dimensions of	Dimensions of privacy: privacy as integrity of the individual (includes privacy of personal	Dimensions of privacy: The guidance discusses privacy only in terms of data protection. (A

[47] A workstream means a project, policy, proposal, initiative, etc.
[48] MOJ Guidance, p. 12.
[49] MOJ Guidance, p. 4.

privacy, stakeholders, legal and social reference points?	information, privacy of person, privacy of personal behaviour and privacy of personal communications) Stakeholders: Here, these include groups or organisations interested, involved or affected by the project. An outline list is provided (Part II, Ch III, p 28). Legal reference point: Provides an indicative list of potentially relevant laws protecting privacy rights (See Part II, Chapter VI) . Public needs, expectations and concerns: growing awareness of privacy, losses of personal data; concern about information collection; privacy risks (to individuals and organisations); issues involving identification.	PIA's function is to identify and address data protection risks.) Stakeholders: here are "interested parties" – the guidance suggests that organisations thoughtfully choose a "wide range of stakeholders" from bodies such as civil liberty groups, other government departments, regulatory bodies, third sector bodies, legal specialists and specific representative groups. Legal reference point: The Data Protection Act 1998 Public needs, expectations and concerns: Data protection issues; concerns regarding processing of personal data.
Stakeholder engagement – early contact with stakeholders, information provision, consultative process, early conduct of consultative process, communication of process and outcomes, exposure to draft PIA report and publication of final PIA report.	Calls for early identification of and preliminary talks with key stakeholders; addresses information provision requirement; encourages wide and continuous engagement with stakeholders; recommends writing a PIA report with "the expectation that it will be published, or at least be widely distributed" (see Part II, Chapter IV).	Early consultation with stakeholders; consulting stakeholders is described as a "core element" of PIA. Outlines two steps of consultative process; envisages, as the Data Handling Review advocates, the provision of periodic reports (PIA reports) which may be published or distributed to stakeholders.
Orientation – process cf. product; solutions cf. problems	Views PIA as a process; outlines constructive solutions (means to avoid and mitigate privacy risks – privacy impact avoidance and mitigation measures).	Stresses overtly PIA as process. Calls for solutions to problems, but does not detail what they might be.
The PIA process Does it describe the preliminary privacy issues analysis process? Does it outline phases or structure? Does it provide sufficient detail about activities within	Provides a description of preliminary privacy issues analysis. Provides an outline of phases in a PIA.	Re description of preliminary privacy issues analysis, it outlines initial screening process. Provides outline of phases/structure.

each phase? Does it lead an organisation to move the outcomes forward through the design and implementation phases? Does it give guidance on the contents of a PIA report?	Provides detail about phase activities. Stresses moving outcomes forward in design and implementation. Provides guidance on PIA report contents. Outlines, in terms of functions (reasons), key elements and sources of content for report.	Provides detail about activities in the different PIA phases, although more succinctly than the ICO Handbook. Moves outcomes forward in design and implementation (in section on "Tying up loose ends"). Lists the various aspects to cover in PIA reports.
Role of the oversight agency	Specifies that the ICO has no formal role in conduct, approval or signing off the PIA report.	Does not mention the role of an oversight agency.

7.5 LEGAL BASIS

1. General framework for privacy and data protection

As a member of the Council of Europe, the UK ratified the ECHR and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). It also signed but has not ratified the Additional Protocol (ETS 181). As a member of the EU, the UK is bound by the Charter of Fundamental Rights (with restrictions)[50] and the EU data protection framework.

The UK does not have a written constitution. The Human Rights Act 1998 gives further effect to the ECHR. A right of privacy is not explicitly provided for in domestic legislation, but it hasslowly emerged in case law.[51]

The basic data protection legal instruments in the UK are the **Data Protection Act 1998** and the **Privacy and Electronic Communications (EC Directive) Regulations 2003**. Section 6 of the Act established the Information Commissioner's Office (ICO).[52] The ICO is responsible for data protection in England, Scotland, Wales and Northern Ireland.

2. Laws on PIA forerunners

In the implementation of the 1995 Data Protection Directive, section 22 of the Data Protection Act 1998 ("Preliminary assessment by Commissioner") provides for a form of **prior checking**:

> (1) In this section "assessable processing" means processing which is of a description specified in an order made by the Secretary of State as appearing to him to be particularly likely –
> (a) to cause substantial damage or substantial distress to data subjects, or
> (b) otherwise significantly to prejudice the rights and freedoms of data subjects.

[50] Cf. Protocol No. 30 to the TEU and TFEU.
[51] Privacy International, *Privacy and Human Rights 2006. Country Reports – United Kingdom of Great Britain and Northern Ireland*, 2007. https://www.privacyinternational.org/article/phr2006-united-kingdom-great-britain-and-northern-ireland
[52] Information Commissioner's Office. http://www.ico.gov.uk

(2) On receiving notification from any data controller under section 18 or under notification regulations made by virtue of section 20 the Commissioner shall consider –
(a) whether any of the processing to which the notification relates is assessable processing, and
(b) if so, whether the assessable processing is likely to comply with the provisions of this Act.

(3) Subject to subsection (4), the Commissioner shall, within the period of twenty-eight days beginning with the day on which he receives a notification which relates to assessable processing, give a notice to the data controller stating the extent to which the Commissioner is of the opinion that the processing is likely or unlikely to comply with the provisions of this Act.

(4) Before the end of the period referred to in subsection (3) the Commissioner may, by reason of special circumstances, extend that period on one occasion only by notice to the data controller by such further period not exceeding fourteen days as the Commissioner may specify in the notice.

(5) No assessable processing in respect of which a notification has been given to the Commissioner as mentioned in subsection (2) shall be carried on unless either—
(a) the period of twenty-eight days beginning with the day on which the notification is received by the Commissioner (or, in a case falling within subsection (4), that period as extended under that subsection) has elapsed, or
(b) before the end of that period (or that period as so extended) the data controller has received a notice from the Commissioner under subsection (3) in respect of the processing.

(6) Where subsection (5) is contravened, the data controller is guilty of an offence.

(7) The Secretary of State may by order amend subsections (3), (4) and (5) by substituting for the number of days for the time being specified there a different number specified in the order.

3. PIA legal bases

No explicit basis for PIA in the laws of the UK has been found.

However, following the high profile loss of data by HM Revenue and Customs, in June 2008, the Cabinet Office issued a policy document *Data Handling Procedures in Government: Final Report*.[53] It requires that a PIA is conducted on large-scale IT systems:

> Section 3: Implementation
> 3.9. From July: … Privacy Impact Assessments will be used and monitored.

The Report, in its executive summary, states also:

> This report describes how Government has now put in place new measures to protect information, to apply across central Government. No organisation can guarantee it will never lose data, and the Government is no exception. But the actions in place:
> …

[53] Cabinet Office, *Data Handling Procedures in Government: Final Report*, June 2008. http://www.cabinetoffice.gov.uk/resource-library/data-handling-procedures-government

- reinforce efforts to ensure that civil service working culture supports the proper use of information. This applies both at the planning stage through use of Privacy Impact Assessments and when services are being delivered.

The Cabinet Office is the department responsible for co-ordinating policy across the UK central Government and promoting efficiency. Its guidance does not have legal force but sets out the policy which all government departments are expected to follow. The Cabinet Office monitors this policy. The ICO is not involved, as it is not a requirement of the Data Protection Act. Therefore, this obligation can be considered only as soft aw.

4. Guidance material

In 2007, the Information Commissioner's Office (ICO) issued a PIA handbook. A revised version was published in 2009.[54] It is considered as a landmark PIA document in the UK. In 2010, a PIA guide was issued by the Ministry of Justice.[55]

In 2010, a document on PIA procedure was issued by Ridgeway Partnership, an NHS [National Health Service] trust providing specialised health and social care.[56]

In April 2010, pursuant to the new section 41C of the Act, the ICO issued the "Assessment notices code of practice".[57] Regarding PIA-like initiatives, the Information Commissioner's Office issued a manual on data protection audit in June 2001.[58]

5. Proposals

In June 2008, the Coleman Report,[59] an independent review on how public authorities handle and protect the information they hold, recommended that Government:

7. Tackle identity management challenges through mandating the use of privacy impact assessments. Specify standards of protection for identity registration, management and use in government and the wider public sector.

The Select Committee on the Constitution of the House of Lords issued in 2009 a report on surveillance.[60] Having assessed the concept of PIA (see paras 293-306), the Committee stated:

[54] Information Commissioner's Office, *Privacy Impact Assessment Handbook Version 2.0*, 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

[55] Ministry of Justice, *Undertaking Privacy Impact Assessments: The Data Protection Act 1998*, 2010. http://www.justice.gov.uk/guidance/docs/pia-guidance-08-10.pdf.

[56] Ridgeway Partnership, *Procedure for completing a Privacy Impact Assessment*, Version 1.0, 2010. http://www.ridgeway.nhs.uk/client_media/medialibrary/2010/10/Privacy_Impact_Assessment_Procedure.pdf

[57] Information Commissioner's Office, *Assessment notices code of practice*, 2010. http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/assessment_notices_code_of_practice.pdf

[58] Information Commissioner's Office, *Data Protection Audit Manual*, June 2001. http://www.privacylaws.com/Documents/External/data_protection_complete_audit_guide.pdf

[59] *Protecting Government Information – Independent Review of Government Information Assurance (The Coleman Report)*, commissioned by the Cabinet Office, June 2008. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/colemanreport.pdf

[60] House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State. 2nd Report of Session 2008–09*, Vol. 1. http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/18.pdf

317. We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these PIAs. We also recommend that the Government – after public consultation – consider introducing a similar system for the private sector.

7.6 COMMENTS ON THE SHORTCOMINGS AND EFFICACY OF PIA IN THE UK BY PIA EXPERTS

PIA experts Adam Warren and Andrew Charlesworth outline the shortcomings and efficacy of PIA in the UK.[61] In terms of efficacy, they think the UK PIA system is a "policy success".[62] They state:

> The ICO has clearly worked very hard, both in public and behind the scenes, to promote the use of PIAs; to seek and utilise feedback to make the handbook more user friendly; and to encourage government agencies which have undertaken PIAs to make their reports public.[63]

Clarke describes the UK ICO Handbook as one of the "best practice publications".[64] It falls into the category of high quality guidance documents when evaluated against the criteria he proposes (i.e., status of the guidance document, discoverability, applicability, responsibility for the PIA, timing of the PIA, scope of the PIA, stakeholder engagement, orientation, the PIA process and the role of the oversight agency).[65]

Despite this, Warren and Charlesworth contend that there are several problems with the UK PIA system. One issue is the lack of a UK government order for "preliminary assessment" despite the government's having identified three probable cases of processing that might be covered under its scope (data matching, processing involving genetic data and processing by private investigators).[66] This is in contrast to other EU Member States that have put checks in place in relation to sensitive data, offences and criminal convictions, and genetic data.[67] Warren and Charlesworth recommend that the UK address its lack of meeting the requirement of "prior checking"[68] through the wider use of PIAs.

Another shortcoming highlighted by Warren and Charlesworth is the lack of review and oversight. They stress that even

> the Ministry of Justice does not itself review departmental PIA processes or reports, and may not be informed when PIAs are undertaken. As such, detailed data protection responsibilities, including establishing PIA processes, are routinely devolved to individual departments. There

[61] Warren, Adam, and Andrew Charlesworth, "Privacy Impact Assessment in the UK" in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
[62] Ibid.
[63] Warren and Charlesworth, op. cit., 2012.
[64] Clarke op. cit., 2011. Note, Clarke was lead author on the team that drafted the Information Commissioner's 2007 PIA Handbook.
[65] Ibid.
[66] Warren and Charlesworth, op. cit., 2012.
[67] Citing ICO, *Privacy Impact Assessments: international study*…, Appendix H, pp. 5-9. See also Le Grand, Gwendal, and Emilie Barrau, "Prior checking, a forerunner to privacy impact assessments" in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].
[68] As envisaged under Article 20 of the EU Data Protection Directive.

> does not currently appear to be any central co-ordination of officials or civil servants with PIA experience across government departments; any central guidance as to the type of projects that would fall within the "mandatory" PIA requirement; or any central guidance on appropriate or approved consultants.[69]

Warren and Charlesworth find the "focus on departmental responsibility" (note our earlier discussion of the MOJ Guidance),[70] the "apparent lack of PIA cross-fertilization across departmental boundaries" and the "relatively 'hands-off' oversight" raise doubts about the efficacy of governmental PIA processes.[71] They further highlight the problems with departmental responsibility for its own PIA processes: disregard of privacy failures arising directly from executive decisions, disregard of issues that are not under the specific remit of one particular department and the disregard of cumulative effects of programmes initiated by different departments upon the individual. [72]

They also point out that there is no formal process of external review of PIAs in the UK by central agencies or by the ICO (which functions largely as an advisory body in this respect).

The next problem highlighted by Warren and Charlesworth is a "PIA skills gap".[73] In this respect, they particularly suggest that departments be encouraged to "share PIA tools, templates and frameworks".[74]

Warren and Charlesworth also highlight the "inward-facing" use of PIAs to inform management risk assessments.[75] PIAs conducted by government departments are less "public-facing" – attributed to the ICO's emphasis on self-assessment and lack of focus on generating documentation for public review. This has made obtaining information about PIAs and their outcomes difficult.

Warren and Charlesworth note that, in the UK, as in other places, there is:

- no consistent process for ensuring effective consultation with stakeholders, notably the general public, e.g., a register of ongoing PIAs, consultation periods and relevant contact details;
- no consistency in reporting formats for PIAs, whether in draft or completed, e.g., a PIA might be reported in a detailed 62-page document, or simply mentioned in a paragraph in a general impact statement[76]; and,
- no strategy for ensuing that, where PIA decisions and reports are made publicly available, they are easily accessible, perhaps from a centralised point, e.g., the UK Office of Public Sector Information (OPSI) or the ICO.[77]

[69] Warren and Charlesworth, op. cit., 2012.
[70] Section 1.3
[71] Warren and Charlesworth, op. cit., 2012.
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] See, for example: Department of Communities and Local Government, *Making Better Use of Energy Performance Data: Impact Assessment*, Consultation, March 2010.
http://www.communities.gov.uk/documents/planningandbuilding/pdf/1491281.pdf. Department for Transport, *Impact Assessment on the Use of Security Scanners at UK Airports*, Consultation, March 2010.
http://www.dft.gov.uk/consultations/closed/2010-23/ia.pdf
[77] Warren and Charlesworth, op. cit., 2012

Therefore, Warren and Charlesworth advocate the development of a "coherent approach to PIA consultation and dissemination".[78]

Elsewhere, Warren, Bayley et al., also highlight further issues,[79] such as the perception amongst project managers that PIAs are a burden, internal stakeholder resistance, wariness of engagement with external stakeholders and PIA publication. They also note that the ICO "did not have resources to validate PIAs and that civil society groups, in particular, were often too time-pressured – and also lacked the resources – to contribute to the process".[80] In this respect, they make some suggestions such as identifying linkages between PIAs and policy-making, improved stakeholder engagement, greater use of technologies and possible partnerships with the private sector.

Clarke has also commented on the shortcomings of UK PIA, particularly the UK ICO Handbook. In his analysis of international PIA guidance documents,[81] he states that the ICO Handbook has the following issues: first, its scope of applicability is unclear; second, it fails to convey that PIAs are mandatory for government agencies; and third, the MOJ Guidance that makes data protection the primary focus of PIAs undermines its value.

Wright highlights how, "In the U.K., there is currently no formal Parliamentary backing for PIAs, and the ICO can only recommend their completion."[82] Further, he highlights that, despite Cabinet Office assurances of PIA usage in all departments, "there is no reporting mechanism in place whereby, for example, a government department is obliged to inform ICO of the PIA or the Treasury in making submissions for funding programs."[83]

7.7 BEST ELEMENTS

Outlined below are the best elements of the two UK Guidance documents.

ICO Handbook, 2009

- The ICO Handbook, more than any other PIA guidance, emphasises the importance of engaging stakeholders in the PIA process.
- It emphasises PIA as a process, not simply an exercise aimed at producing a report.
- It recognises that there is no "one size fits all" PIA – organisations are to use the Handbook to guide their PIA process in a manner "appropriate to their circumstances".[84]
- It emphasises a broad scope of application for PIAs. This is evident in its use of the term "project" to include not only the activities and functions of the assessed organisation but also to refer to systems, databases, programs, applications, services or

[78] Warren and Charlesworth, op. cit., 2012
[79] Warren, Adam P, Robin Bayley, Colin Bennett, Andrew Charlesworth, Roger Clarke and Charles Oppenheim, "Privacy Impact Assessments: The UK Experience", 31st International Conference of Data Protection and Privacy Commissioners, Madrid, 4-6 November 2009. https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/5783/3/SDPA_paper_1009fnl.pdf.
[80] Ibid., p. 6.
[81] Clarke, op. cit., 2011.
[82] Wright, David, "Should Privacy Impact Assessments be Mandatory?" *Communications of the ACM,* Vol.54, No. 8, August 2011, pp. 121-131 [p. 127]
[83] Ibid.
[84] ICO Handbook, op. cit., p. 2.

schemes, an enhancement to any of the above, initiatives, proposals or reviews, or draft legislation.

- It stresses the early commencement and conduct of a PIA.
- It makes a clear distinction between a PIA and privacy or data protection audits.
- It advises that the PIA process inform or be embedded as part of the consultative process of public sector projects, many of which are obliged to consult stakeholders, including the public. It promotes PIAs as both good governance and good business practice. It also clearly assigns responsibility for a PIA (making clear the commitments required in terms of PIA accountability).
- It sets out the end results of an effective PIA – this is helpful in any post-PIA evaluation.
- It interprets privacy in a holistic manner – i.e., in terms of the integrity of the individual. It recommends that PIAs take into account four essential types of privacy: of personal information, of the person, of personal behaviour and of personal communications.
- It outlines privacy, risks, impacts and vulnerabilities alongside means or options for addressing them (acceptance of risks, privacy impact avoidance measures and privacy impact mitigating measures).
- It provides detailed textual and graphical guidance to illustrate the PIA process.
- In addition to providing comprehensive guidance for a PIA, it also provides guidance on where to find further information and other sources of help and advice.
- It not only lists the screening questions, but also accompanies them with related interpretation.
- Its Appendices contain useful templates such as the Data Protection Compliance Checklist, the Privacy and Electronic Communications Regulations Compliance Checklist, the PIA screening questions and privacy strategies.

MOJ Guidance 2010

- The MOJ Guidance is very specific in nature and limited to application of the DPA 1998 (processing of personal data).
- It stresses consultation of stakeholders as a “core element”.
- It conceptualises the PIA process as a “living” document.

8 UNITED STATES

In the United States, privacy impact assessments for government agencies are mandated under the E-Government Act of 2002. This Act states that PIAs must be conducted for new or substantially changed programmes which use personally identifiable information. Personally identifiable information (PII) is defined as "any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a U.S. Citizen, Legal Permanent Resident, or a visitor to the U.S."[1] The processing of PII in the US is also covered by Fair Information Practice Principles (FIPP) from the Privacy Act of 1974. These include the following eight principles: transparency, individual participation, purpose specification, minimisation, use limitation, data quality and integrity, security and accountability and auditing. However, because this legislation only pertains to the federal public sector, there is a marked difference in the use of PIAs and other official privacy protections between the public and private sectors. In consequence, this chapter will focus on the use of PIAs in the public sector where they are officially mandated.

8.1 ANALYSIS OF EXISTING PRIVACY IMPACT FRAMEWORK

While the Privacy Act of 1974 provided some protections for individuals and consumers regarding the processing of personal information, in 2002, a number of information security laws were enacted to better protect personal information, particularly as it is processed by the government. The Federal Information Security Management Act (FISMA) and the E-Government Act of 2002 both introduced further protections for individuals whose information is processed, and the latter included a mandate for government agencies to conduct privacy impact assessments. The subsequent creation of new agencies, such as the Department of Homeland Security, further entrenched and expanded this use of PIAs by introducing a Chief Privacy Officer role with responsibility for conducting PIAs. However, as will be noted below, this has led to a significant mismatch between the rules governing public sector use of PIAs and other privacy measures and private sector use of those tools.

Although not directly related to privacy impact assessments, FISMA addresses the protection of personal information through defining federal requirements for security information and the associated information systems which support federal agency operations. It states that agencies must develop information security programmes, and extend these to contractors or other providers of information systems. According to the Government Accountability Office (GAO), information security under FISMA "means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy".[2] Consequently, FISMA represents a requirement to protect information once it has been collected, whereas the PIA process described in the E-Government Act requires agencies to consider whether personal information needs to be collected in the first place.

[1] Department of Homeland Security, *Privacy Technology Implementation Guide*, 16 Aug 2007, p. 8.
[2] Government Accountability Office, *Homeland Security: Continuing Attention to Privacy Concerns is Needed as Programs Are Developed*, GAO-07-630T, 21 Mar 2007, p. 7.

The E-Government Act was signed by the President on 17 Dec 2002 and became effective on 17 April 2003. Section 208 of the Act requires federal agencies to conduct a privacy impact assessment, which must be reviewed by a chief information officer or equivalent official, and should be made public, unless it is necessary to protect classified, sensitive or private information contained in the assessment. Finally, agencies are expected to provide their Director with a copy of the PIA for each system for which funding is requested. Each agency Director must issue guidance to their agency specifying the contents required of a PIA, and this guidance must ensure that the PIA is "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information".[3]

Additionally, the creation of the Department of Homeland Security (DHS) via the Homeland Security Act of 2002 mandates that the DHS conduct privacy impact assessments and creates a Chief Information Officer position with responsibility for these privacy assessments. Therefore, unlike other agencies where privacy compliance has been added to their overall mission, the notion of privacy protection was intended to be embedded within the structure of the DHS from the start.

Private sector

The role of PIAs in relation to private sector organisations has been mixed. While some companies, such as Microsoft, are using PIAs alongside privacy officers, other private sector organisations are resistant to the use of PIAs or to using the PIA guidance promulgated by the federal public sector. Bamberger and Mulligan note that in relation to the private sector, private firms, sometimes with Federal Trade Commission (FTC) guidance, have shifted their understanding of privacy protections from procedural protections (notice and consent) to risk management strategies that avoid harms that are caused by the misuse of consumer data.[4] Colin Bennett also states that although corporations may not be calling their risk assessment processes PIAs, it is probable that the "assessment of privacy implications has been an integral part of new product and service review for many companies for a long time…[and that] just because there are few instruments called PIAs published within the US corporate sector, does not mean that equivalent risk assessments are not performed".[5] Bennett further notes that many of these assessments are proprietary.

However, Roger Clarke's evaluation is much more negative, particularly in relation to the use of public consultation in privacy impact processes. He argues that some organisations are seeking to "forestall legislative provisions" for PIAs by creating and supporting industry standards. While a US standard in the form of an American National Standards Institute standard (2004) and an International Standards Organisation (ISO/IEC JTC-1 SC-27 WG-5) standard are in place, Clarke argues that "these processes have lacked the least vestige of consultation with people, or with their representatives or advocates for their interests."[6] In relation to public consultations in general, Clarke further notes that "the ideology of the US private sector is hostile to the notion that consumers might have a participatory role to play in

[3] E-government Act of 2002 , Pub.L.107-347.
[4] Bamberger, Kenneth A., and Deirdre K. Mulligan, "Catalyzing Privacy: New Governance, Information Practices, and the Business Organization", *Law & Policy*, 2011 [forthcoming], p. 2.
[5] Bennett, Colin J., "Appendix D: Jurisdictional Report for United States of America", *Privacy Impact Assessments: International Study of their Application and Effects*, Information Commissioner's Office, Wilmslow, UK, Oct 2007, p. 3.
[6] Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", C*omputer Law & Security Review*, Vol. 25, No.2, April 2009, pp. 123-135 [p. 128]. PrePrint at http://www.rogerclarke.com/DV/PIAHist-08.html

the design of business systems. This is of considerable significance internationally, because US corporations have such substantial impact throughout the world."[7]

Public sector

These laws have led to a discrepancy between the PIA provisions undertaken in the federal public sector and the private sector in the US. While PIA in the US is certainly less developed than in some other countries, privacy officers, in some form, have been used in the public sector for some time. Many federal agencies have had privacy officers, or Privacy Act officers, for a number of years, although in some agencies, this has been a part-time job.[8] Despite the existence of these officers, many do not spend much time on privacy issues specifically, but instead deal with subject access requests from individuals who wish to view their records under the terms of the Privacy Act or access information under the Freedom of Information Act. According to Dempsey, despite the existence of these officers, "They are often mid-level career officials and do not have the ability to intervene at a policy level even when a major privacy issue comes to their attention. They are often brought into discussions about a program only at the last minute to draft a notice required under the Privacy Act when the government creates or changes a 'system of records,' but that notice generally serves no role in shaping policy."[9] Despite this, Dempsey states that a few federal government privacy officers have been some of the most innovative in the world across both the public and private sectors.[10]

The Internal Revenue Service, US Postal Service, Commerce Department and Department of Homeland Security all have privacy officers or individuals in similar roles, and PIA is one of the tools at their disposal. PIAs form a significant part of the privacy compliance process. Federal agencies, as part of the E-Government Act, are supposed to make PIAs publicly accessible and post them publicly. Dempsey argues that while the PIAs that have been made publicly available are of high quality, the number of agencies making their PIAs publicly available is not yet adequate.[11] Many public sector organisations also publish privacy impact assessment guides to assist their employees in preparing a PIA.[12]

In addition to the federal public sector, some state governments and state and local agencies have been requiring PIAs for some time.[13] Blair Stewart, in his chapter in the forthcoming book *Privacy Impact Assessment*, says that the New York Public Service Commission may have been one of the first regulators to require a PIA in 1991.[14] Similarly, California has been discussing introducing PIAs for some time; however, this has not been implemented as yet.[15] The following sections discuss two PIA guidance documents produce by federal public agencies to illustrate how PIAs are conceptualised and used in the US.

---

[7] Clarke, op. cit., 2009, p. 128.
[8] Dempsey, James X., Statement before the House Committee on the Judiciary Subcommittee on Commercial and Administrative Law, "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security", 10 February 2004.
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Department of Homeland Security, *Privacy Technology Implementation Guide*, 16 Aug 2007.
[13] See Annex 2 for some details re the legal basis for PIA in Ohio, as an example.
[14] State of New York Public Service Commission, *Privacy Policy Statement No. 1: A Privacy Impact Statement* in "Statement of Policy on Privacy in Telecommunications", 22 March 1991, reprinted in Longworth Associates, *Telecommunications and Privacy Issues: Report for the Ministry of Commerce*, Wellington, 1992.
[15] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, Issue 2, May 2011, pp. 111-120. http://idpl.oxfordjournals.org/content/1/2.toc

8.1.1 Office of Management and Budget

On 26 Sept 2003, the Office of Management and Budget (OMB) issued a Memorandum to heads of Executive departments and agencies providing guidance for implementing the privacy provisions of the E-Government Act, as required by section 208 of the Act.[16] The OMB is responsible for providing guidance on privacy and information policy in the US and Bennett argues that it is a "central agency" in relation to PIA policy.[17] Unfortunately, this important Memorandum is very difficult to find on the OMB website, as it is only listed under memoranda, and thus an individual would need to do a key word search for the memo or would have to know what year the memorandum was issued.

The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are required to conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available. PIAs should also be performed or updated when changes to an existing system create new privacy risks, and the OMB guidance provides nine examples of such situations.[18] Agencies must also update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form. Government contracts "that use information technology or that operate websites for purposes of interacting with the public" or "relevant" cross-agency initiatives should also be the subject of a PIA. However, no PIA is required where information relates to internal government operations, where it has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged.

The OMB defines PIA as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."[19] Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The OMB specifies what must be in a PIA and, in doing so, it puts an implicit emphasis on the end product, the report, rather than on the process of conducting a PIA. Regarding the **content of a PIA**, it says PIAs must analyse and describe:

1. what information is to be collected (e.g., nature and source);
2. why the information is being collected (e.g., to determine eligibility);
3. intended use of the information (e.g., to verify existing data);
4. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);

[16] Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Washington, DC, 26 Sept 2003. http://www.whitehouse.gov/omb/memoranda/m03-22.html
[17] Bennett, op. cit., 2007.
[18] See http://www.whitehouse.gov/omb/memoranda/m03-22.html for a list of these examples.
[19] OMB, op. cit., 2003.

5. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorised uses), and how individuals can grant consent;
6. how the information will be secured (e.g., administrative and technological controls); and
7. whether a system of records is being created under the Privacy Act.

Furthermore, the guidance states that the PIA requires an analysis of the privacy issues and solutions examined, not simply a statement of them. For example, a PIA conducted at the IT development stage should address privacy in the documentation associated with the development of the systems. This should include a statement of need, a functional requirements analysis, an alternatives analysis, feasibility analysis, benefits/cost analysis and an initial risk assessment. A development stage PIA should also address the impacts that the system will have on individual privacy, and specifically identify and evaluate threats related to each of the seven facets of the content of the PIA as discussed above. The PIA should also include an assessment of the solutions or choices made as a result of conducting the PIA. For example, in relation to development stage PIAs, the OMB states that the PIA may need to be updated before deployment of the system to reflect new information or choices made as a result of the initial PIA analysis. The OMB also states that PIAs conducted for major information systems should reflect an extensive analysis of:

1. the consequences of collection and flow of information,
2. the alternatives to collection and handling as designed,
3. the appropriate measures to mitigate risks identified for each alternative and
4. the rationale for the final design choice or business process.

Furthermore, the depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.

Agencies must consider the information life cycle (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. The OMB guidance sees collaboration by different stakeholders, although it does not specifically say that different stakeholders should include stakeholders external to the agency: "To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy."[20]

PIAs must be approved by a "reviewing official", e.g., the agency's chief information officer, other than the official procuring the system or the official who conducts the PIA. Only then is it submitted to the OMB. The PIA document is to be made publicly available. However, agencies are not obliged to make the PIA or a summary publicly available if publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest). Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. Reports must state for which

[20] OMB, op. cit., 2003.

information technology systems or information collections PIAs were conducted, the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all, and if in summary form or not at all, agencies must explain their choice.

8.1.2 Homeland Security

The Department of Homeland Security is another major agency which publishes PIA guidance for those seeking to undertake a PIA. This document has undergone a number of revisions, and the most recent version which is discussed here is the 2010 version. This document is easier to locate than the equivalent OMB guidance, as an interested individual can browse for it. However, the document is available three pages into the website and an individual would have to look under the department structure, then the Office of the Secretary and then the Privacy Office if they wished to locate the document. This placement makes it quite difficult to find and somewhat unintuitive.

One of the key facets of the DHS PIA programme is the specific inclusion of an independent, high ranking internal privacy officer. The Homeland Security Act of 2002 established a privacy officer within the DHS, and this was the first federal statutory privacy officer position in the US. The remit of the privacy officer is to ensure that the use of technology for homeland security "sustains and does not erode privacy protections"; to ensure compliance with the Privacy Act of 1974; to evaluate legislative and regulatory proposals involving personal information and to conduct PIAs.[21] The authority to conduct PIAs is also part of the Homeland Security Act under section 222.

The requirement to conduct a PIA depends upon the collection of personally identifiable information (PII). The DHS Guidance helpfully distinguishes between PII and private information, where, "Private information is information that an individual would prefer not be known to the public because it is of an intimate nature. Personally identifiable information is much broader; it is information that identifies a person or can be used in conjunction with other information to identify a person, regardless of whether a person would want it disclosed. If the information or collection of information connects to an individual, it is classified as 'personally identifiable information.'"[22] The Department of Homeland Security Act states that the DHS Privacy Officer should also conduct a PIA in situations where one is not required by the E-Government Act, for example, in respect of proposed department rulemaking, to ensure that new rules do not adversely affect privacy, for national security systems, to ensure that such secret programmes appropriately consider and implement privacy protections and for human resources information systems.[23]

According to the DHS PIA guidance, a PIA should accomplish two goals. First, it should determine the risks of using an electronic information system to collect, maintain and disseminate PII and, second, it should evaluate the protections and alternative processes for handling this information identified by the organisation to mitigate potential privacy risks. As a result, the guidance describes the PIA as a "living document", which needs to be updated

[21] Bamberger, Kenneth, and Deirdre Mulligan, "PIA requirements and privacy decision-making in US government agencies" in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, London, 2012 [forthcoming].
[22] Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance*, June 2010, p. 5.
[23] Teufel III, Hugo, *Privacy Policy and Guidance Memorandum*, Department of Homeland Security, Memorandum Number 2008-02, 30 Dec 2008.

regularly as systems and processes are changed and updated. Here, the DHS appears to focus on PIA as a process, rather than an end result.

The use of a PIA as a form of public engagement is cited in a number of paragraphs in the PIA guidance document. The document states that the DHS privacy officer has "broad authority to identify and comment on privacy matters resulting from proposed Departmental rules, regulations, and technologies and *to do so in a public manner* (emphasis added)".[24] In theory, this provision gives the chief privacy officer considerable leverage in ensuring that PIAs are conducted properly. The guidance also states that the PIA will help the public to understand DHS information collection activities, including what information is being collected, why the information is being collected, how the information will be used, how the information will be accessed and how it will be stored. According to the document, privacy impact assessment is "one of the most important instruments through which the Department creates transparency and establishes public trust in its operations".[25] Therefore, it is the public nature of PIAs which is integral to one of its primary functions.

PIAs perform other functions as well. They assist in informed-decision making for the department in that they help managers identify privacy issues and evaluate whether they have been adequately addressed.[26] In addition to the transparency element mentioned above, the PIA contributes to accountability. PIAs also provide a benchmark to enable Congress, the GAO and the OMB to evaluate privacy compliance within the DHS.

Under DHS guidance, privacy impact assessments are not automatic. A PIA is only conducted when "developing or procuring any new technologies or systems that handle or collect personally identifiable information… The PIA should show that privacy was considered from the beginning stage of system development."[27] PIAs will also need to be conducted if an organisation modifies an existing system, updates its existing collections or decides to collect new information. The presence of PPI triggers the use of a Privacy Threshold Analysis (PTA) that is used to determine if a full PIA is required. A PTA requires the evaluator to undertake the following steps[28]:

1. Describe the project;
2. State from whom information is collected;
3. State whether it utilises Social Security Numbers;
4. State what information is collected/retained/generated
5. State whether the new system is an infrastructure project (LAN vs. Wide Area Network). If so, state whether it creates logs of information;
6. State whether the system connects, receives or shares personally identifiable information;
7. State whether there is a Certification & Accreditation record within the Office of the Chief Information Officer's (OCIO) Federal Information Security Management Act (FISMA) tracking system.

Finally, if a PIA is found to be required for a system that is being developed, the pilot of that system must have the PIA completed prior to launch of the pilot.[29]

[24] DHS, *Privacy Impact Assessments*, 2010, p. 2.
[25] DHS, *Privacy Impact Assessments*, 2010.
[26] Teufel, 2008.
[27] DHS, *Privacy Impact Assessments,* 2010, p. 6.
[28] Department of Homeland Security, *Privacy Threshold Analysis Template*, 10 June 2010.
[29] DHS, *Privacy Impact Assessments*, 2010, p. 7.

The PIA guidance notes and the associated PIA Template[30] describe the components of a DHS PIA. A PIA begins with an abstract that describes the project in three or four sentences. This is followed by eight different sections, beginning with an **overview** which "creates the foundation for the entire PIA".[31] The overview should discuss the context and background information necessary to understand the purpose and mission of the project and a justification for the privacy sensitive elements. The overview will discuss what legal authority enables the collection of information by the project, what System of Records Notice (SORN)[32] applies to the information and describes a system security plan for the information systems which support the project. The overview also describes the project's relationship with other administrations and acts, including the National Archives and Records Administration and the Paperwork Reduction Act.

Section 2 of the PIA is a **characterisation of the information collected** that defines and describes the scope of the information requested or collected and the reasons for its collection. This section includes specific questions about the source of the information, the specific information that is requested, whether the information is publicly available data, and how the accuracy of the information is ensured. Finally, this section also requires a privacy impact analysis related to the characterisation of the information, whereby the scope and intended use of the information requested is matched to the fair information practice principles, including the principles of purpose specification, minimisation, individual participation and data quality and integrity.

Section 3 describes **how the information will be utilised** by the project. This includes a discussion of how and why the project is using the information, whether the project will mine the data (i.e., whether it will use the technology to conduct electronic searches or attempt to discover or locate a predictive pattern or associated anomalies), whether there are other components of the system that will use the information and a privacy impact analysis of the principles of transparency and use limitation.

Section 4 requires that officials discuss the issues of **notice and consent**. This section seeks information about the notice to individuals about the information collected, their right to consent to the use of their information and the right to decline to provide information. In this section, the provisions for *prior* notice and consent are explained. However, for some projects, particularly those related to national security, notice is not given and consent or the possibility of opting out is not provided. In these cases, officials must justify why the project is exempt from these requirements. Finally, officials must conduct a privacy impact analysis related to notice, including a discussion of the principles of purpose specification, minimisation, individual participation and data quality and integrity.

Section 5 explores the aspects of **data retention by the project**. In this section, officials must explain why and how long information is retained. Officials must also conduct a privacy

[30] DHS, *Privacy Impact Assessment Template*, 2010.
[31] DHS, *Privacy Impact Assessments*, 2010, p. 11.
[32] A SORN includes the following: "Name and location of the system; Categories of individuals on whom records are maintained in the system; Categories of records maintained in the system; Each routine use of the records contained in the system, including categories of users and purpose of such use; Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; Title and business address of the agency official responsible for the system of records; Agency procedures whereby an individual can be notified at his or her request if the system of records contains a record pertaining to him or her; Agency procedures whereby an individual can be notified at his or her request how he or she can gain access to any record pertaining to him or her contained in the system of records, and how he or she can contest its contents; and Categories of sources of records in the system." Bennett, op. cit., 2007, p. 2.

impact analysis related to retention, including a discussion of the principles of data minimisation and data quality and integrity.

Section 6 describes the **sharing of information** outside of the DHS, including sharing project information with other federal, state and local government and/or private sector entities. Questions in this section include whether information is shared outside of DHS as part of normal agency operations. If so, officials must identify those organisations and describe how the information is accessed and utilised. This section also questions how the sharing is compatible with the associated SORN and whether there are limits on re-dissemination once the information is shared. Officials must also explain how they will maintain records of disclosures of information outside the department. Finally, they must conduct a privacy impact analysis of the sharing of information and describe how privacy will be ensured once the information is shared. This could include the use of a memorandum of understanding or some other mechanism.

Section 7 focuses on processes through which individuals can seek **redress**. These processes could include systems which allow individuals to access the records held about themselves, ensure the accuracy of the information held about them and to file complaints. Again, some projects will be exempt from this requirement if it is sensitive to national security, but this must be explained in full. In this section, officials must describe the procedures in place to allow individuals to access their information and correct inaccurate information. Officials must also describe how the project notifies individuals about the procedures for correcting information. Finally, officials must conduct a privacy impact analysis of the principle of individual participation.

The final section, Section 8, discusses **auditing and accountability**. In this section, officials must describe the technical and policy-based safeguards and security measures that ensure that project information is used in accordance with the practices stated in the PIA. Officials are required to describe privacy training provided to users and to discuss the procedures for ensuring that only authorised users have access to the information. Finally, this section asks how the project will review and approve changes to the mechanisms described in the PIA, including changes to the use of information, access to the system, information sharing agreements and new memoranda of understanding.

A completed PIA should be signed by the component privacy office for approval and then submitted to the department privacy office. If no component privacy office exists, the PIA can be submitted directly to the DHS privacy office. Upon receipt, the DHS privacy office places the document in a queue for review. Once reviewed, the privacy office will outline steps for document finalisation and publication.

According to the guidance, PIAs should be made publicly available as mandated by the E-Government Act. The guidance states that PIAs should be understandable to the general public, although the length and breadth of the report should vary according to the size and complexity of the project. Making the report publicly available demonstrates that the system has privacy protections built in, which were the result of an in-depth analysis.[33]

Unlike other agencies, the DHS has an external oversight body that evaluates PIAs and other privacy activities. This oversight body is the result of work by the first DHS privacy officer,

[33] DHS, *Privacy Impact Assessments*, 2010, p. 9.

Nuala O'Connor Kelly, who "leveraged her status and independence so as to play a singular role in the creation of the Data Privacy and Integrity Advisory Committee (DPIAC)".[34]

8.2 LEGAL BASIS

1. General framework for privacy and data protection

There is no explicit right to **privacy** in the US Constitution. The Supreme Court has ruled that there is a limited constitutional right of privacy based on several provisions in the Bill of Rights.[35]

The **Privacy Act of 1974**[36] establishes a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in systems of records by federal agencies.[37] The US has no comprehensive privacy protection law for the private sector. A patchwork of federal laws covers some specific categories of personal information, e.g., the Children's Online Privacy Protection Act of 1998 (COPPA).[38] There is no independent federal privacy oversight body, but every federal agency is required to appoint its own privacy officer (Sec. 552 of the Consolidated Appropriations Act of 2005). The Office of Management and Budget (OMB) plays a limited role in setting policy for federal agencies under the Privacy Act of 1974.[39]

2. Laws on PIA forerunners

No explicit basis for any PIA-like tool in the laws of the United States has been found.

3. PIA legal bases

The **E-Government Act of 2002**[40] is a comprehensive legal instrument enacted "to enhance the management and promotion of electronic Government services and processes" in the US by "establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services". For these purposes, it created the Office of E-Government and Information Technology[41] within the Office of Management and Budget (OMB).

The Act also deals with privacy protection and its section 208(b) explicitly provides for PIA be conducted:

> (1) RESPONSIBILITIES OF AGENCIES.

[34] Bamberger and Mulligan, "PIA requirements and privacy decision-making in US government agencies", 2012 [forthcoming].
[35] Privacy International, *Privacy and Human Rights 2006. Country Reports – United States of America*, 2007. https://www.privacyinternational.org/article/phr2006-united-states-america
[36] Privacy Act of 1974, 5 USC 552a, amended. http://www.justice.gov/opcl/privstat.htm
[37] Department of Justice, Office of Privacy and Civil Liberties. http://www.justice.gov/opcl/privacyact1974.htm
[38] Children's Online Privacy Protection Act of 1998, Pub.L. 105-277, 15 USC §§ 6501-6506. http://www.ftc.gov/ogc/coppa1.htm
[39] Privacy International, *Privacy and Human Rights 2006. Country Reports – United States of America*, 2007. https://www.privacyinternational.org/article/phr2006-united-states-america
[40] E-Government Act of 2002, Pub.L. 107-347, 44 USC 36. http://www.gpo.gov:80/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (official source).
[41] Office of E-Government & Information Technology. http://www.whitehouse.gov/omb/e-gov

(A) IN GENERAL. – An agency shall take actions described under subparagraph (B) before –
(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
(ii) initiating a new collection of information that –
(I) will be collected, maintained, or disseminated using information technology; and
(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) AGENCY ACTIVITIES. – To the extent required under subparagraph (A), each agency shall –
(i) conduct a privacy impact assessment;
(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) SENSITIVE INFORMATION. – Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) COPY TO DIRECTOR. – Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT. –

(A) IN GENERAL. – The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) GUIDANCE. – The guidance shall –
(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
(ii) require that a privacy impact assessment address –
(I) what information is to be collected;
(II) why the information is being collected;
(III) the intended use of the agency of the information;
(IV) with whom the information will be shared;
(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
(VI) how the information will be secured; and
(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ‘‘Privacy Act’’).

(3) RESPONSIBILITIES OF THE DIRECTOR. – The Director shall –
(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;
(B) oversee the implementation of the privacy impact assessment process throughout the Government; and

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

Sec. 222 of the **Homeland Security Act of 2002** explicitly provides for PIA be conducted:

> The Secretary shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including
> ...
> (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected.

4. Guidance material

Pursuant to Sec. 208(b)(2)(A) of the E-Government Act of 2002 ("The Director shall issue guidance to agencies") and section 208(b)(3)(A) thereof ("The Director shall develop policies and guidelines for agencies"), a substantial number of PIA guidance materials has been issued. In 2003, the Office of Management and Budget (OMB), a presidential executive office, issued a memorandum on "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002".[42]

In June 2010, the Department of Homeland Security issued its own PIA guidance material pursuant to *both* Sec. 208(b) of the E-Government Act of 2002 and Sec. 222 of the Homeland Security Act of 2002.[43]

Other guidance material include the following:

- Department of Defence (2009): *DoD Instruction 5400.16 – DoD Privacy Impact Assessment (PIA) Guidance*[44]
- Defense Information Systems Agency (DISA) (2007): *DISA Privacy Program Instruction 210-225-2*[45]
- Department of Justice (2010): *Privacy Impact Assessment Guidance*[46]
- Department of Justice (2010): *Initial Privacy Assessment (IPA) Instructions & Template*[47]
- Department of Justice – Office of Justice Programs (2009): *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives*[48]
- Securities and Exchange Commission (2007): *Privacy Impact Assessment (PIA) Guide*[49]
- Office of Personnel Management (2010): *Privacy Impact Assessment (PIA) Guide (Version 2.0)*[50]

[42] Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22. http://www.whitehouse.gov/omb/memoranda_m03-22
[43] Department of Homeland Security, *Privacy Impact Assessments. The Privacy Office Official Guidance*. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf
[44] Cf. http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf
[45] Cf. http://www.disa.mil/about/legal/pia
[46] Cf. http://www.justice.gov/opcl/pia_manual.pdf
[47] Cf. http://www.justice.gov/opcl/initial-privacy-assessment.pdf
[48] Cf. http://www.ojp.gov/BJA/pdf/PIAGuide-Feb09.pdf
[49] Cf. http://www.sec.gov/about/privacy/piaguide.pdf
[50] Cf. http://www.opm.gov/privacy/PIAs/PIAGuide.pdf

- Department of the Interior (2004): *Privacy Impact Assessment and Guide*[51]
- Department of Health and Human Services – National Institutes of Health (2010): *NIH Privacy Impact Assessment (PIA) Guide*.[52]

8.3 AUDITS BY THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Independent, third-party assessment of PIAs in the US government agencies are made by OMB reports to Congress and the GAO. Unfortunately, the data for some of these assessments is self-reported by government agencies, leading to contradictions between the self-reported data and data generated as a result of GAO investigations.

The US federal goal is for all major federal agencies to implement robust PIA policies and for 100 per cent of applicable systems to publicly post PIAs. In 2010, all 24[53] of the major federal agencies reported that they had written policies for the following elements of PIAs:

- Determining whether a PIA is needed;
- Conducting a PIA;
- Evaluating changes in technology or business practices identified during the PIA process;
- Making PIAs available to the public as required by law and OMB policy;
- Monitoring the agency's systems and practices to determine when and how PIAs should be updated; and
- Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained.[54]

Furthermore, 23 of the 24 agencies reported written policies on:

- Determining circumstances where the agency's Web-based activities warrant additional consideration of privacy implications; and
- Making appropriate updates and ensuring continued compliance with stated Web privacy policies.[55]

Federal agencies are falling short of their target of 100 per cent of systems having publicly posted PIAs. In 2008, 92 per cent of applicable systems had publicly posted PIAs, while in 2009, this figure dropped to 89 per cent (although this was accompanied in a rise in systems requiring a PIA in 2009). In the 2010 fiscal year report, this figure had increased to 93 per cent of all systems that required a PIA.[56] While this does not yet meet the 100 per cent target, it shows some improvement.

However, the self-reported nature of the data has resulted in some discrepancies. For example, the FISMA reporting guidance asks agency inspectors to rate the quality of each agency's PIA process. In 2009, self-reported data from the 25 major federal agencies included in an OMB report to the US Congress indicated that 23 of the agencies had "developed and documented

[51] Cf. http://www.doi.gov/ocio/privacy/pia.htm
[52] Cf. http://oma.od.nih.gov/ms/privacy/NIHPIAGuide.doc
[53] In 2010, the GAO reported that there were 24 major federal agencies, while in its reports of 2008 and 2009, there were 25 as the Department of the Treasury was counted twice. There is no associated explanation.
[54] Office of Management and Budget, *Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*, 2010, p. 30.
http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf
[55] Ibid.
[56] Ibid.

an adequate policy for PIAs".[57] Yet, the inspectors of only 14 of those agencies with "adequate policies" reported that these polices were fully implemented and under operation.[58] Consequently only 56 per cent of these federal agencies were actually operating an adequate PIA policy.[59]

According to Bamberger and Mulligan, "these self-reported figures mask deeper qualitative non-compliance issues with the PIA mandate". For example, in a review of data mining applications by five different federal agencies, the GAO found that only three of the five agencies examined had carried out a PIA (although one was exempt), and that "none of these assessments adequately addressed all the statutory requirements".[60] Specifically, the IRS, Small Business Administration and Risk Management Agency PIAs did not adequately address the statutory requirements regarding their data mining efforts and the FBI conducted no PIA, in violation of agency regulations. This violation of statutory requirements included a failure to ensure that the PIA was reviewed by the agency's chief information officer or equivalent and a failure to identify the choices made by the agency as a result of undertaking the PIA. Furthermore, in only two cases was the PIA made fully publicly available. A further GAO report noted a number of failures to comply with privacy requirements for programmes that were covered by the E-Government Act. In particular, the DHS did not conduct a risk assessment of a data mining tool called ADVISE and the DHS failed to provide notice in a programme called "Secure Flight" which collected passenger data prior to boarding on domestic flights.[61] According to the GAO:

> The lack of comprehensive assessments is a missed opportunity for agencies to ensure that the data mining efforts we reviewed are subject to the most appropriate privacy protections. Because the assessments did not address all the required subjects, including those related to several Privacy Act provisions, agencies were sometimes unaware that they were not following all the requirements of the act. Further, without analyses regarding their approaches to privacy protection, agencies have little assurance that their approaches reflect the appropriate balance between individual privacy rights and the operational needs of the government.[62]

In relation to the data mining applications, the GAO notes that none of the PIAs addressed the choices that the agency made once privacy issues were uncovered in the data mining operations. Therefore, there is no documentation of the basis for the choices they made to address both privacy protections and operational needs.[63] GAO reports have also documented a highly "uneven" compliance on basic Privacy Act requirements.[64] In 2011, the GAO was still advising a number of different agencies, including but not limited to the Department of Agriculture, the Secretary of Veterans' Affairs and the Secretary of State to carry out PIAs to

[57] Office of Management and Budget, *FY 2009 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, 2009, p. 23.
http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf
[58] OMB, op. cit., 2009, p. 22.
[59] Bamberger and Mulligan, "PIA requirements and privacy decision-making in US government agencies", 2012 [forthcoming].
[60] Government Accountability Office, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866, Aug 2005, p. 25.
http://www.gao.gov/new.items/d05866.pdf
[61] GAO, op. cit., 2007, pp. 10–15.
[62] GAO, op. cit., 2005, p. 27.
[63] Ibid., p. 28.
[64] Government Accountability Office, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304, June 2003, p. 14. http://www.gao.gov/new.items/d03304.pdf

examine how individual personal information is accessed and used in these agencies' interactions with individuals on social media.[65]

8.4 COMMENTS ON THE SHORTCOMINGS AND EFFICACY OF PIA IN THE US BY PIA EXPERTS

The issues uncovered in audits by the GAO demonstrate a number of shortcomings inherent in the US PIA system as it is currently designed and implemented. PIA experts have identified three different specific shortcomings of the US PIA: its lack of public consultation mechanisms, the compliance only orientation of the process and, relatedly, the fact that the PIA is a living document in name only. However, despite these shortcomings, privacy experts have also noted that the US PIA does effectively assist in considering privacy in the public sector and enables agencies to work towards improvements in their system design.

A lack of public consultation mechanisms when undertaking a PIA is one of the primary shortcomings PIA experts identified in respect of US PIAs. Bamberger and Mulligan note that although the E-Government Act requires agencies to produce a PIA before developing or purchasing new technology systems and requires public publication of the PIA document, there is no provision within the Act for public consultation during the production of the PIA.[66] According to these authors, such a "lack of explicit mechanisms for public participation in the PIA process…limits the opportunities for outside experts to assist the agency in identifying the privacy implications of often complex technological systems".[67] As a result, Bennett notes that it is very rare for individuals outside the agency to comment upon a PIA before it is published.[68]

Furthermore, Dempsey notes that the OMB has encouraged agencies not to publish PIAs until after their budgets are finalised, leading to a retrospective evaluation of the PIA itself, which, as Dempsey argues, "is inconsistent with the purpose and value of PIAs" and fails to encourage public participation in debates around privacy concerns.[69] This makes it difficult for members of the public to express their concerns around new technology systems and exercise their democratic voice in encouraging lawmakers to reject proposals for new systems. According to Bamberger and Mulligan, the end result has been that Congress itself has not actively engaged in monitoring privacy-related decisions, and that there is a danger that changes to systems as a result of privacy considerations will consist of small adjustments at the margins of systems rather than abandonment or overhaul of those systems.[70] Bennett concludes that although the publication of PIAs does contribute to transparency, the lack of prior consultation with either experts or members of the public can harm the legitimacy of new technology systems and the PIA process.[71]

---

[65] Government Accountability Office, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO 11-605, 29 June 2011. http://www.gao.gov/new.items/d11605.pdf

[66] Bamberger and Mulligan, "PIA requirements and privacy decision-making in US government agencies", 2012 [forthcoming].

[67] Bamberger, Kenneth A., and Deirdre K. Mulligan, "Privacy Decisionmaking in Administrative Agencies", *University of Chicago Law Review*, Vol. 75, No. 1, 2008, pp. 75-107 [p. 87]. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1104728

[68] Bennett, op. cit., 2007.

[69] Dempsey, op. cit., 2004.

[70] Bamberger and Mulligan, "PIA requirements and privacy decision-making in US government agencies", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

[71] Bennett, op. cit., 2007, p. 11.

PIA experts have also concluded that PIAs in the US often function as a compliance activity rather than a reflexive process of continually considering the privacy implications of technology or information systems. Roger Clarke argues that this compliance orientation is related to the guidance note associated with the E-Government Act of 2002 that limits the assessment to compliance checks as do many agencies' own internal guidance documents.[72] Bennett has expressed concerns that while there is a significant number of PIAs published by US federal agencies as a result of the legislative mandate, they are of variable quality and some agencies appear to engage in a "checklist approach" that treats a PIA as something that they have to do as part of their annual budget review, rather than something they should do.[73] In relation to the DHS use of a privacy threshold analysis (PTA) to determine whether a PIA is necessary, Roger Clarke offers a scathing critique, arguing that the PTA examination is "so superficial, and so unrelated to actual privacy needs and expectations, that extraordinarily privacy-invasive measures were instituted in a wide range of systems".[74] Accordingly, US federal agencies conduct PIAs "in name only" and despite rare exceptions, the US "remains a wasteland from the viewpoint of privacy policy".[75] Clarke concludes that government agencies have subverted PIAs to a legal compliance study and private corporations do not adequately address privacy issues, which has serious implications due to their privileged position in the global economy.[76] In consequence, Bennett states that there is a general consensus among US privacy advocates that it is better to require that PIAs are conducted and published than not, but that questions remain over whether such internal procedures regarding privacy risks result in significant changes.[77]

The final major criticism directed at PIAs in the US is that they are a living document in name only. This is related to the criticism above in that both critiques are related to a lack of reflexive analysis of the privacy risks and solutions presented within the PIA. For example, a compliance-focused PIA places more emphasis on producing a PIA report as a compliance activity. Therefore, there is no revisiting of the privacy issues through the lifetime of the project. Bennett notes that in contrast to DHS and US Postal Service PIA activities, the IRS PIA policy appears to place more emphasis on the *process* of conducting a PIA rather than the document which is the outcome.[78] Similarly, Rotenberg argues that when a PIA is conducted by the DHS, they are required to ensure that potential privacy-infringing practices are identified, but they are not required to resolve these issues.[79] In another example, Bennett notes that although agencies must have privacy compliance documentation in place before approaching the OMB for funding, there is no evidence of budgets being sent back for review due to insufficient or incomplete PIA documentation.[80] However, despite these robust criticisms, the PIA process in the US does effectively offer some consideration of privacy issues for federal agencies.

Bennett argues that, despite some serious criticisms, "PIAs have stood out as one of the more positive aspects of American privacy protection policy within the last ten years."[81] Rotenberg

[72] Clarke, op. cit., 2011, p. 117.
[73] Bennett, op. cit., 2007, p. 12.
[74] Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", C*omputer Law & Security Review*, Vol. 25, No. 2, April 2009, pp. 123-135 [p. 128]. http://www.rogerclarke.com/DV/PIAHist-08.html
[75] Ibid.
[76] Clarke, op. cit., 2009, p. 130.
[77] Bennett, op. cit., 2007, p. 13.
[78] Bennett, op. cit., 2007.
[79] Rotenberg, op. cit., 2006.
[80] Bennett, op. cit., 2007, p. 7.
[81] Bennett, op. cit., 2007, p. 11.

concurs, stating that the PIA framework is similar to a multi-step analysis of security systems and "provides a systematic way of evaluating not only the privacy risks of a given system but also the efficacy of the system in achieving its intended purpose." [82] He states that a PIA can enable an analysis of the scope, the legal basis and efficacy of the system as well as the effect of the system on privacy interests. Testimony from one of the DHS Chief Privacy Officers, Hugo Teufel III, re-affirms the value of PIAs that help agencies understand how the use of personal information affects privacy and states that "we made a policy decision to complete a PIA for many programs under the authority of Section 222 of the Homeland Security Act, even when one is not required under the E-Government Act".[83]

However, a number of experts have argued that this efficacy is dependent upon the institutional infrastructure and the timing of the PIA. In relation to the institutional infrastructure, Bennett argues that the presence and type of privacy infrastructure within an agency may be the most important influence on whether conducting PIAs is successful for an organisation.[84] Bamberger and Mulligan, as well as Dempsey, have highlighted the ways in which the Department of Homeland Security has implemented one of the more robust PIA practices of the major US federal agencies, and the structure of the privacy office within the DHS is one of the primary reasons for this robustness. Bamberger and Mulligan identify three factors that contribute to successful implementation of PIA in US government agencies: "(1) the status and independence of a privacy expert embedded within the agency; (2) the decentralised distribution, disciplinary diversity, prior experience, and expertise of the privacy staff; and (3) the creation of an alternative external oversight structure, which [in the case of the DHS] proved particularly significant given the lack of systematic congressional and administrative privacy oversight".[85] Dempsey's testimony to the US Congress is largely in agreement, although he further argues that the statutory basis of a privacy officer or privacy office and the privacy officer's inclusion in senior-level policy deliberations is an essential element of an effective privacy office.[86] Bennett agrees, stating that "these conditions are generally considered necessary for the advancement of privacy protection policies in general and PIAs in particular".[87]

In respect of the independence of a privacy officer or privacy office, Bamberger and Mulligan argue that independence in action and reporting is an essential element of effective government data protection offices. They cite a number of scholarly sources and official testimony to support this, including an article by Paul Schwartz arguing that an independent data protection body could develop expertise and specialisation currently missing in congressional oversight[88], a book by privacy scholar David Flaherty that concludes that independent agency oversight is the key to ensuring that a data protection law works in

[82] Rotenberg, Marc, "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11", Social Science Research Network, Sept. 2006, pp. 24-25. http://ssrn.com/abstract=933690

[83] Department of Homeland Security, "Testimony of Hugo Teufel III, Chief Privacy Officer, U.S. House of Representatives Committee on the Judiciary, Subcommittee on Commercial and Administrative Law", 27 July 2007. http://www.dhs.gov/xnews/testimony/testimony_1185548980016.shtm

[84] Bennett, op. cit., 2007, p.1.

[85] Bamberger and Mulligan, "PIA requirements and privacy decision-making in US government agencies", 2012 [forthcoming].

[86] Dempsey, op. cit., 2004.

[87] Bennett, op. cit., 2007, p. 13.

[88] Schwartz, Paul, "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer", *Hastings Law Journal*, Vol. 43, 1992, pp. 1379–84 [pp. 1380-1381].

practice[89], a 1987 article by Spiros Simitis which asserts that efficient regulation presupposes an independent control authority[90] and the 1973 report by the US Department of Health, Education and Welfare that recognises that agency oversight would be the strongest option for protecting privacy but that this suggestion was rejected due to lack of political support.[91] Dempsey further notes that the independence of the chief privacy officer and his or her position outside the formal power infrastructure of the organisation was key to ensuring a responsive PIA process for the DHS US-VISIT PIA.

In relation to the staff available to a privacy officer or to undertake PIAs, Bennett argues that PIAs are more likely have a greater impact on agency culture, if specialised personnel "who not only know about the law and the technology, but can forcefully articulate the larger ethical and moral questions" are present within the agency.[92] Dempsey, of the Center for Democracy and Technology, concurs, stating that one of his organisation's key understandings of what makes an effective privacy officer and subsequent effective PIA policies is the presence of adequate staff to support those activities.[93] In another piece, Bamberger and Mulligan cite interviews with privacy officials to argue that robust privacy protections are assisted by integrating a network of specially trained employees into business lines in order to address privacy concerns during the design phase of projects.[94]

Experts also agree that PIAs are especially effective if they are "pre-decisional", in that they are published before the system design or regulatory process is completed.[95] Although Bennett critiques the lack of opportunity for public consultation in relation to published PIA documents, he agrees that the pre-decisional nature of PIA processes does allow for a significant amount of internal review and analysis.[96]

Experts have also argued that PIAs are an effective instrument to increase public trust and confidence. According to Teufel, publicly posting PIA documents not only helps the DHS identify and mitigate privacy concerns, but also enhances public confidence in the steps the DHS has taken to protect individual privacy alongside security.[97] Dempsey agrees, stating that the existence of a privacy officer "participating in senior level policy deliberations …[and] using the tools of Privacy Act notices and Privacy Impact Assessments, can be an important mechanism for raising and mitigating privacy concerns" about the government's use of personal information.[98]

Given these points of considerable efficacy, the following section extracts some of the best elements of the US PIA process as recommendations for a European PIA framework.

---

[89] Flaherty, David H., *Protecting Privacy in Surveillance Societies,* University of North Carolina, Chapel Hill, 1989, p. 381.
[90] Simitis, Spiros, "Reviewing Privacy in an Information Society", *University of Pennsylvania Law Review*, Vol. 135, No. 3, 1987, p. 742.
[91] US Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, 1973, pp. 42-43.
[92] Bennett, op. cit., 2007, p. 12.
[93] Dempsey, op. cit., 2004.
[94] Bamberger and Mulligan, "Catalyzing Privacy: New Governance, Information Practices, and the Business Organization", *Law and Policy*, Vol. 33, 2011 [forthcoming], p. 13.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701087
[95] Dempsey, op. cit., 2004.
[96] Bennett, op. cit., 2007, p. 13.
[97] DHS, op. cit., 2007.
[98] Dempsey, op. cit., 2004.

8.5 BEST ELEMENTS

In conclusion, experience from the US suggests a number of recommendations for a European PIA framework. These include a recommendation that:

- A chief privacy officer or a privacy office has independence within the organisation.
- The chief privacy officer has a senior position within the organisation and participates in high-level deliberations.
- A chief privacy officer, privacy office and/or PIA process be statutorily mandated by an external agency.
- There is external oversight over the privacy officer, privacy office or PIA process.
- An adequate number of specially trained privacy focused staff members be embedded throughout the organisation.
- Comprehensive PIAs should be produced early in the process of introducing a technology or system in order to assess and mitigate the privacy impacts.
- PIAs should be publicly available and posted on an agency's website so as to increase transparency and public confidence.
- PIA guidance include a specific template to guide and assist staff in producing comprehensive PIA reports.

9 TEN EXAMPLES OF PRIVACY IMPACT ASSESSMENT REPORTS

PIA reports are rather difficult to find, especially those conducted by the private sector. Roger Clarke has said that, in addition to the PIAs conducted by government departments and agencies, "PIAs have been conducted in the for-profit and not-for-profit sectors, but are still not widespread. Few have been widely publicised, and the author is aware of no published reports. Areas in which projects are known to the author to have been conducted include toll-roads, transport ticketing, consumer e-commerce applications and participant authentication in health records systems. Coles-Myer, the Australian retail chain, was reported in 2006 as having applied the IPPs to a project to produce a data warehouse relating to retail customers."[1]

Tancock, Pearson and Charlesworth found that, in the UK, some 270 PIAs have been conducted by government department and agencies as of January 2010, according to a Cabinet Office report.[2]

Clarke reported that the British Columbia registry of PIA summaries numbered about 150 at the end of 2007.[3] Clarke himself has listed exemplars of PIA reports in Appendix 2 of his article "Privacy Impact Assessment: Its Origins and Development", published in April 2009.

For example, although they are supposed to be posted on US government department websites, in fact, this does not happen as often as it should. The GAO has criticised government departments for not carrying out PIAs when they should have done. One of the authors of this proposal has attempted to get a PIA from a UK government department, but was told that a Freedom of Information request would be necessary to obtain a copy, even though the UK Information Commissioner's Office has called upon government departments to engage stakeholders in the preparation of PIAs and the Cabinet Office has made performance of PIAs mandatory (as is the case in Canada).

Consultants have performed many PIAs (one said he had conducted more than 30), in some cases for companies as well as government departments. None of the PIAs for companies have been made public and many of those for government agencies have also not been made public. One of the authors of this proposal has conducted PIAs for the private sector and in one instance only the company decided to make the PIA public.

Case studies of existing privacy impact assessments are helpful in identifying strong points as well as shortcomings in how PIA has been implemented. Lessons can be learned and good practice identified.

Bamberger and Mulligan cite examples of PIAs in the US as short as one and a half pages.

---

[1] Clarke, 2012.

[2] Tancock, David, Siani Pearson and Andrew Charlesworth, "Analysis of Privacy Impact Assessments within Major Jurisdictions", in *Proceedings of the 2010 Eighth Annual International Conference on Privacy, Security and Trust*, Ottawa, 17-19 Aug 2010, published 30 Sept 2010, pp. 118-125 [p. 121]. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5593260. The cited Cabinet document is Cabinet Office, "Protecting Information in Government", 10 Jan 2010, p. 14. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/caboffprotectinfo.pdf

[3] Clarke, 2011, p. 127.

Some PIA examples demonstrate how the process can vary for different project types or for projects at different stages.

It is hard to find published examples of PIA reports. So far as we know, this report is the first to provide an analysis of existing, published PIA reports. We have compiled a list of PIA reports and chosen 10 from that list, two from each of Australia, Canada, New Zealand, the UK and the US. We've chosen PIA reports on diverse topics prepared by diverse authors and/or enterprises. We would certainly advocate more empirical research and analysis of existing PIAs, not only to review their structure, approach, efficacy and shortcomings, but also to examine their length and detail, which would help provide more evidence of how long it takes to conduct a PIA, who conducted the PIA, etc.

9.1 CRITERIA INDICATING THE EFFECTIVENESS OF A PIA REPORT

We assess the effectiveness of a PIA report against the following core criteria (while recognising that other criteria could be included[4]). The PIA report should:

- clarify whether the PIA was initiated early enough so that there was still to influence the outcome
- who conducted the PIA
- include a description of the project to be assessed, its purpose and any relevant contextual information
- map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)
- check the project's compliance against relevant legislation
- identify the risks to or impacts on privacy
- identify solutions or options for avoiding or mitigating the risks
- make recommendations
- be published on the organisation's website and be easily found there or, if the PIA report is not published (even in a redacted form), there should be an explanation as to why it has not been published
- identify what consultation with which stakeholders was undertaken.

Even if a PIA report met all of the above criteria, it does not necessarily mean that the PIA process itself was effective. For example, the PIA might have been initiated early, but the organisation that undertook the PIA might have viewed the whole exercise merely as "window-dressing" and had no intention of seriously engaging with stakeholders and addressing the recommendations. Even if the organisation did take the PIA process seriously, it might be that the assessor, the leader of the PIA process, was not very experienced and did not conduct a good PIA process. Or, some stakeholders might have been consulted, but it might have been only a limited number and only those known to support the project.

9.2 AUSTRALIA – ELECTRONICALLY VERIFYING IDENTITY

The Attorney-General's Department (AGD) asked Information Integrity Solutions Pty Ltd (IIS) to conduct a PIA on a proposal to amend the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) to authorise the use and disclosure of credit reporting information for electronic identity verification (EV). EV involves checking

[4] See, for example, "Clarke, Roger, "Privacy Impact Assessment Guidelines", Xamax Consultancy Pty Ltd, 10 February 1998, revised 25 August 1999. http://www.xamax.com.au/DV/PIA.html

specified identity details – at a minimum, name, address and date of birth or transaction history – against information held by other organisations.

The AGD proposed that credit reporting information held by credit reporting agencies (CRAs) could be used and disclosed for EV under tightly prescribed arrangements and with associated privacy protections. A reporting entity would be able to send identification information provided by a customer to a CRA for a data match. A CRA, in receipt of such a request from a reporting entity, would be limited to confirming the accuracy of the information provided to them. This may be done through either a 'yes/no' system or a scoring system. The score would depend on how closely the information provided by the reporting entity matches with the customer information held on the credit file.

Reporting entities have to decide how much checking is needed to be satisfied that the customer in a transaction does not pose an unacceptable risk of money-laundering or other identified threats.

The Government decided to allow the proposed amendments to the AML/CTF Act to proceed, subject to appropriate privacy protections.

Information Integrity Solutions (IIS) is a consultancy based in New South Wales, Australia, providing services to government agencies, companies and not-for-profit organisations. It has provided services in the information privacy field since 2004. Its principals include Malcolm Crompton, former Australian Privacy Commissioner.

According to its website, IIS has conducted PIAs for federal and state government departments and agencies. IIS says its approach to PIA builds on guidelines issued by the Australian Office of the Privacy Commissioner and by the UK Information Commissioner's Office. It goes beyond compliance with privacy law to look at the wider privacy challenges including allocation of risks and individual trust and looks for solutions so that information flows are appropriate and to everyone's benefit.

IIS has a fact sheet on how it conducts PIAs.[5] Key phases of this process include:

- *Information gathering* – The result of this phase is a description of the project and its information flows and the purpose of collection, use and disclosure of personal information.
- *Analysis* – This phase assesses the project against privacy principles. In addition, IIS looks at other privacy risks that an organisation should address to better achieve consumer confidence and trust in the product, service or new process.
- *Consultation* – This phase enables an organisation to present information about a project to stakeholders and to gain input at an early stage. It says good consultation can generate a sense of ownership, trust and understanding amongst stakeholders.
- *Recommendations and report* – based on the analysis and input from the consultation, IIS provides recommendations in its PIA reports about how to allocate and mitigate individual privacy risks.

IIS says it aims to create an electronic environment which inspires individual confidence, trust and willingness to engage. To achieve this, when conducting its PIA analysis, IIS considers

[5] "The IIS Approach to Privacy Impact Assessments".
http://www.iispartners.com/Services/index.html#privacyImpact

how an organisation can use four key tools to help build positive privacy solutions into its projects:
Law – Is the legal framework right? Does it properly promise enforceable protection?
Technology (its design and implementation) – Is technology being deployed in a way that enhances the protection of personal information and delivers organisational policy and legal obligations?
Governance – What governance frameworks are in place to ensure that the promises of business process, technology platforms and legal obligations are actually being met?
Safety-Net – What is in place when something goes wrong to ensure that individuals do not bear a disproportionate level of risk given that they are the party least able to manage, mitigate or bear it?

The purpose of the PIA on electronic identity verification was to assess the privacy impacts of the Attorney-General's Department's proposal and to take into account the views of stakeholders.

At the behest of the AGD, IIS undertook the PIA and prepared a 55-page PIA report[6] consisting of nine sections, including an Executive Summary, an Introduction, Description of the proposal and other background, Personal information collection and information flows, Privacy issues and risks, Findings and recommendations, and three appendices listing reference documents, parties consulted for this PIA and consultation questions.

IIS describes (p. 4) the methodology it followed in preparing its PIA report for the Attorney General's Department, which is basically that outlined in its fact sheet referenced above. This included considering compliance with the privacy principles in the Privacy Act 1988, in particular, the provisions relating to credit reporting. It also considered the broader privacy risks, including how these are allocated between reporting entities, credit reporting agencies (CRAs) and citizens. The PIA followed these main steps:

- Information gathering
- Analysis of the information to identify impacts on privacy
- Consultation with key stakeholders. The consultation process involved:
  - Contacting stakeholders, providing them with a short consultation paper and inviting them to a meeting and/or to provide submissions by 21 August 2009 (submissions received are listed at Appendix 2 of the IIS report); and
  - Conducting a series of meetings in the period 5-10 August 2009, also listed in Appendix 2.
- Developing a draft report and recommendations which were provided to AGD and then to stakeholders who had previously provided submissions or attended meetings with request for comments by 29 September 2009. Following consideration of these comments and discussions with AGD, IIS developed the final report.

IIS commented that the EV proposal had been crafted so as to minimise privacy impacts, including by minimising changes to the credit reporting system. Nevertheless, it identified (p. 5) various privacy risks if identity information held by credit reporting databases were made available for AML/CTF EV, including these:

[6] Information Integrity Solutions, "Privacy Impact Assessment Report: Electronically Verifying Identity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Using Credit Reporting Information, Prepared for the Attorney General's Department", 8 Oct 2009.
http://www.iispartners.com/Services/index.html#privacyImpact

- "function creep" meaning that the proposal extends the use of credit reporting data beyond that currently permitted by the law and expected by the community, potentially undermining community trust in credit reporting and, for example, willingness to consider other changes to the credit reporting system;
- the potential for the identity confirmation process to create new data about individuals that could then be used for new purposes, with or without the knowledge of the individual concerned which may or may not be to the advantage of the individual;
- the potential for individuals to be disadvantaged if they "fail" the EV process should it involve the use of credit reporting information, for example, because of inaccuracies in the information held by CRAs or because of the nature of the checking process, without inadequate advice or recourse;
- the extent of choice that individuals have in the process, for example about whether to provide paper documents in a face-to-face identity verification process or to proceed with electronic verification and if the latter to choose whether or not to have credit reporting information included as part of an EV check; and
- the extent to which CRAs or reporting entities might either incidentally or otherwise gain access to personal information beyond what is necessary for the purposes of identity verification for AML/CTF purposes and who bears the risk when problems or mistakes with electronic verification system arise.

In developing its recommendations, IIS says it drew on its "layered defence" approach, by applying a number of possible "tools" to arrive at solutions. These tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves.
- Additional law where risks are particularly high (e.g., specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability;
- Safety-net mechanisms for citizens when failures or mistakes occur.

IIS made 14 recommendations to minimise privacy risks. It recommended that enabling legislation should address issues of consent, permit reporting entities in seeking EV using credit reporting information to provide only an individual's name, residential address and date of birth to a CRA and that the CRA be permitted to use credit reporting information only to confirm the accuracy of these details, require a CRA to keep a separate record of EV attempts, specify that information obtained or generated as part of EV using credit reporting information must not be used or disclosed for any secondary purpose, among others. It also recommended that the proposal should not proceed unless regulators and dispute resolution bodies are properly resourced to carry out appropriate monitoring of the use credit reporting information in EV processes.

9.2.1 Effectiveness

This PIA report is good. It is quite long (55 pages), detailed, well-structured and well written. It provides a good description of the project and its background. IIS met with and consulted stakeholders. It identified various privacy risks and made a set of recommendations for dealing with those risks. The PIA report includes the consultation questions, which included

some brief background or context for each question. The full report is publicly available. Using our criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
Identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	Yes

9.2.2 Shortcomings

The consultation was rather limited. Only 10 stakeholders were consulted, and only 10 submitted comments on the draft PIA report.

The report is not easy to find on the Web.

9.3 AUSTRALIA – ULTRANET ICT PROJECT FOR SCHOOLS

The Ultranet is a $77 million information and communications technology system being installed in all schools in Australia's Victoria state from the year 2010 by the Department of Education and Early Childhood Development (DEECD). The system offers online access for students and parents to check lessons, homework, results and attendance, as well as collaborative learning spaces in which students and teachers can interact.

Salinger Privacy, a consulting company, conducted a PIA of the design of the Ultranet project, from Sept 2009 to April 2010. The PIA report notes the benefits of the Ultranet, but it also made recommendations to protect the privacy of students and other users. As a result, some significant design changes were made, including removing Facebook-style message walls to address concerns about cyber bullying.

The Victoria government's summary of the PIA report's recommendations and its response is available at http://www.education.vic.gov.au/about/directions/ultranet/security.htm.[7]

On its website, the DEECD points out that the Ultranet is not the same as the Internet. It is described as a closed community with controlled access and with a specific educational

[7] Ultranet Privacy Impact Assessment: Executive Summary and Overview of Recommendations and DEECD Actions. SalingerPrivacy, Privacy Impact Assessment Report:: The Ultranet, Prepared for Victorian Department of Education and Early Childhood Development, Updated August 2010.
http://www.education.vic.gov.au/about/directions/ultranet/security.htm

purpose – to support the learning of students. Once rollout of the system is complete, about 45,000 teachers, 550,000 students and 900,000 parents are expected to use the Ultranet. There will also be approximately 2,000 corporate users from DEECD regional and head offices, as well as around 12,000 non-teaching staff in schools.

The DEECD says the Ultranet includes the following privacy and security protections:

- To access the Ultranet, authorised users must log in with a secure, complex password.
- There are rules around who can access what information, and the types of users that can access each type of 'space' within the Ultranet
- No anonymous postings are possible in the Ultranet – all postings are logged and audited.
- All learning communities on the Ultranet must be moderated by a teacher.
- All users can report inappropriate content.
- In addition to the filtered Internet service available in each school, the Ultranet also contains filters for bad language.

All students, parents, teachers and staff receive user guides outlining their rights and responsibilities in relation to privacy, before they access the Ultranet. The DEECD provides schools with support materials to train staff in privacy matters, and for schools to use with students and parents.

Apart from their name and photograph, only a student's parents and teachers can view their information in the Ultranet. No student contact details, health, medical, behavioural or welfare information are stored on the Ultranet. Teachers have been given clear guidelines on the use of student data in the Ultranet – the only purpose for which they can use the data is when it is necessary to fulfill their official teaching or pastoral care duties to that student. Only legal parents or guardians may access individual student information in the Ultranet. Temporary or long-term suspension of parent access can be arranged in special circumstances to protect individual students.

A parent's name can be viewed in the Ultranet by their child, the teachers at their child's school, and members of community spaces that they choose to join. Parents manage their own information and participation in the Ultranet. Parent contact details are not available in the Ultranet. Parents choose whether or not to participate in community spaces with other parents and teachers in the Ultranet. Where a family is separated, two separate logins can be created so that the parents do not need to see the other's profile. Parents have full control over this process.

Teachers have a profile on the Ultranet. Teachers have full control over their own information and participation in the Ultranet. Teacher contact details are not available to parents, or to students from other schools, in the Ultranet.

Parents are advised to contact their child's school principal if they have any concerns about their privacy or that of their child.

The executive summary of the PIA report (the full report has not been posted on the Internet) is eight pages long (it includes a two-page glossary). It is followed by 10 pages of recommendations made by SalingerPrivacy and the actions taken by DEECD in response.

From the executive summary, we learn that the full PIA report contains the following:

Chapter 1 describes the process and objectives of a PIA, and Salinger's methodology in conducting the PIA. Chapter 2 contains information about the Ultranet's system design, a map of data flows and how personal information will be collected, stored, used and disclosed. Chapter 3 reviews the Ultranet project against Australia's information privacy principles (IPPs), which are listed in Victoria's Information Privacy Act. Salinger also took into account health privacy principles (HPPs), as well as the right to privacy in the Charter of Human Rights and Responsibilities.

As part of its analysis, Salinger posed a set of questions of each IPP, notably:

- Will the project comply with this privacy principle?
- Will the project meet community expectations about this privacy principle?
- What else can be done to minimise risk and maximise protections in relation to this privacy principle, without compromising the project's objectives?

Against each privacy principle, Salinger made recommendations to maximise the privacy enhancing possibilities, and/or minimise the privacy risks of the Ultranet project. Chapter 5 grouped the recommendations in Chapters 3 and 4 under seven themes.

Salinger's executive summary includes a section on findings, where the consultancy found that the Ultranet delivers a significant privacy positive outcome for students, through the easy access afforded to students and their parents to the data held about them in relation to attendance, teacher observations, progress and achievements. It also found some negative privacy impacts – or privacy risks - of the Ultranet, as it was designed. However, it said each of these risks could be mitigated, without significantly affecting the Ultranet's objectives.

Strategies to address these risks included some system design changes, the development of comprehensive materials to communicate with users about their privacy rights and responsibilities to others, and the development of robust policies and procedures to support the Ultranet project. Salinger made 49 recommendations.

One principal recommendation: Salinger suggested development of a single Ultranet User Guide, which would provide guidance on both the technical and normative (appropriate behaviour) aspects to using the Ultranet. The guide would meet the DEECD's legal obligations, but in a format that should be useful and interesting to Ultranet users.

To respond to the risk that some people will be tempted to misuse Ultranet data for their own purposes, Salinger recommended a simple business rule to define legitimate access: "The only purpose for which teachers may use student data from the Ultranet is when it is necessary to enable the teacher to fulfil their official teaching or pastoral care duties to that student."[8] Salinger also recommended a set of access controls, supplemented by transparency and audit logging of access, to enforce that business rule.

To protect the Department from the risk of breaching the 'Direct collection' privacy principle, Salinger recommended that users uploading material to the Ultranet be required to certify that they have the appropriate permission if someone else's personal information is included in the material.

Salinger also recommended development of data retention rules for the Ultranet, and suggested time periods after which data should become "invisible", and periods after which

[8] Ultranet PIA, op. cit., p. 5.

data should be deleted. It recommended that DEECD advise schools to manage requests from any third parties for data from the Ultranet in accordance with the policy relating to law enforcement requests – namely, to ask the third party to put their request in writing, and for the school to then seek advice from either the privacy, legal services, student wellbeing, or conduct and ethics unit of the Department.

Other recommendations included:

- a yearly independent audit of information security
- a clear chain of communication and action in the case of a data security breach
- a post-deployment oversight committee, including the appointment of an Ultranet Privacy Officer or involvement of the DEECD Privacy Unit, and
- publication of its PIA report.

9.3.1 Effectiveness

SalingerPrivacy recommended that its PIA report be published on the DEECD website.

The effectiveness of the PIA report was enhanced by the DEECD identifying the actions it was taking in response to each of the recommendations.

Using our criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes[9]
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	From the executive summary, it's not apparent that any stakeholders were consulted

9.3.2 Shortcomings

The PIA seems not to have questioned the need for the Ultranet – why was such a system deemed necessary?

[9] The responses to this and other criteria questions are based on assumptions, i.e., from a review of the executive summary, it appears that the full report included a description of the project, and so on.

SalingerPrivacy recommended that the report be published on the DEECD website, but only the executive summary was published.

There is no information about consultation with stakeholders in conducting the PIA or preparing the PIA report.

9.4 CANADA HEALTH INFOWAY ELECTRONIC HEALTH RECORDS (EHR)

Infoway is an independent, not-for-profit corporation created by Canada's First Ministers in 2001 "to foster and accelerate the development and adoption of electronic health record (EHR) systems with compatible standards and communications technologies". Funded by the Canadian government, Infoway works with the country's 10 provinces and three territories to implement private, secure EHR systems.[10]

Infoway sponsored a "conceptual" PIA on an EHR "solution" for Canada, which was published in 2008.[11] The 164-page PIA consists of an executive summary and seven chapters which form a "detailed overview" of the "conceptual" PIA plus an annex which is the actual PIA. The chapters consist of an introduction, a description of the EHR "infostructure" and how it works; data flows; privacy law, national policy initiatives and the EHR infostructure; an evaluative framework for assessing the impact of the EHR infostructure on privacy; a privacy analysis; and a conclusion.

The report was prepared by two consultants, Anzen Consulting Inc.[12] and Sextant Software. The report is somewhat tainted by controversy, as Anzen Consulting Inc. was involved in spending scandals in Ontario, which led to the resignation of senior political figures in the Ontario government, including Health Minister David Caplan.[13]

The report starts with a note to readers explaining that "conceptual PIAs" are conducted before all of the details of a system's design are known. "This PIA reflects the privacy risks of the pan-Canadian EHR concept, not of specific developments or implementations." Provinces determine their own approach to EHR development and implementation (and sometimes that approach can be bumpy as Ontario's experience shows).

[10] https://www.infoway-inforoute.ca/lang-en/about-infoway

[11] Anzen Consulting Inc. and Sextant, *A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2*, Canada Health Infoway, 12 Feb 2008. https://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf

[12] Anzen effectively ceased to be when its people were absorbed by Deloitte & Touche LLP in May 2010. http://www.anzen.ca. Prior to its shutting down, Anzen principals were touched by controversy over billing practices in Ontario. See Artuso, Antonella, and Jonathan Jenkins, "eHealthy, ewealthy, but wise?", CNews, Canoe.ca, 7 June 2009. The story's "kicker" says it all: "'Incestuous little gang' of consultants making millions". http://cnews.canoe.ca/CNEWS/Politics/2009/06/07/9704751-sun.html. See also CanWest News Service, "Ontario fires eHealth boss over spending scandal", National Post, 8 June 2009. http://www.nationalpost.com/news/story.html?id=1672117

[13] In 2009, Ontario Auditor General Jim McCarter issued a "scathing report on how the province's attempt at electronic health records had loosely spent nearly $1 billion of taxpayer's funds with little to show for it… eHealth [of Ontario] awarded millions of dollars in sole-sourced contracts". Talaga, Tanya, "5 million patients get electronic medical records", *The Toronto Star*, 2 Nov 2010. http://www.thestar.com/news/ontario/ehealth/article/884488--5-million-patients-get-electronic-medical-records

The report's executive summary says that Anzen and Sextant analysed the Blueprint against the 10 privacy principles of the Canadian Standards Association Model Code for the Protection of Personal Information (the CSA Model Code)[14].

This conceptual PIA report seems prone to hype. The detailed overview of the PIA report says that "properly implemented, the EHR Infostructure initiatives currently underway across Canada present an *unprecedented opportunity to bolster privacy*. The analysis concluded that the proposed EHR Infostructure architecture (i.e., the Blueprint Version 2) *strongly supports patient privacy...* Infoway has also *contributed significantly to ensuring that the public is aware of the importance of privacy*" [italics added].[15] Is this PIA report a whitewash?

Infoway "established a Privacy Forum open to representation from all jurisdictions and from both health ministries and Privacy Commissioners/Ombudsmen…for sharing information and experiences so that realistic solutions that support interoperability can be identified".[16]

Chapter 1 of the Overview of the PIA explains (p. 6) that Canada's

> First Ministers agreed to work together to strengthen a Canada-wide health Infostructure and to develop electronic health records and common data standards to ensure the compatibility of health information networks and the stringent protection of privacy, confidentiality and security of personal health information. In response to this agreement, the federal government established Canada Health Infoway Inc. ("Infoway") in January 2001… to foster and accelerate the development and adoption of electronic health information systems with compatible standards and communications technologies. Infoway, whose Members are Canada's 14 federal, provincial and territorial Deputy Ministers of Health, continues to pursue this mission.

In support of its mission, Infoway developed an Electronic Health Record Solution (EHRS) Blueprint ("EHRS Blueprint") as a guide for EHR systems across Canada and to support the secure sharing of health information within and across jurisdictions.

The Overview says (p. 7) that the PIA had four main objectives: (1) to describe the high-level types and flows of personal health information in the EHR; (2) to analyze the EHRS Blueprint against the principles of the CSA Model Code; (3) to identify privacy risks; and (4) to identify mechanisms for enhancing privacy protection.

The PIA (p. 8) looks at the privacy implications of the EHR concept, the EHR Infostructure architecture (as described in the *EHRS Blueprint Version 2* and the PSCA). The report lists the core contents of the PIA:

- The need for the system or initiative that is the subject of the assessment;
- The legislative authority for the system or initiative;
- The personal health information with which the EHR Infostructure deals;
- The sources from which this information is to be obtained;
- The circumstances in which personal health information collection is to take place;
- The intended uses of the personal health information held;
- The proposed recipients of personal health information disclosed and their intended
- use of it;
- The circumstances in which personal health information processing, use and disclosure are to take place;

[14] http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code
[15] Anzen and Sextant, op. cit., p. 4.
[16] Anzen and Sextant, op. cit., p. 5.

- The privacy requirements governing the collection, use and disclosure of the personal health information;
- The safeguards which will be implemented to protect against theft, loss and unauthorised access, use, disclosure, copying, modification or destruction;
- The data protection risks introduced by the system; and
- Observations regarding mitigating strategies.

It also sets out (p. 9) the scope and limits of the PIA. The scope of the PIA includes a discussion of relevant terminology used in the *EHRS Blueprint Version 2,* a description of the working of the EHR Infostructure, a thorough analysis of the EHR Infostructure's impact on patient privacy; and an analysis of the EHR Infostructure's impact on health care provider privacy. The PIA excludes from its scope provincial and territorial implementations of the EHR Infostructure already subjected to PIA; point of service systems in hospitals, physician offices and other health care institutions; privacy practices of health care providers and health care organisations; jurisdictional privacy legislative requirements[17]; issues addressed and resolved by Infoway in its privacy and security use cases, EHR Privacy and Security Requirements or Privacy and Security Standards for the EHR document.

Anzen and Sextant came up with an evaluative framework modelled on the ten principles of the CSA Model Code. The PIA discusses the privacy impacts of the EHR Infostructure based on the framework and makes 29 observations. It also lists Infoway's response to the observations.

Observations (technical and non-technical)[18] were made on inter-jurisdictional data sharing agreements; governance of provider registries; notices concerning EHR infostructures; consent practices; capturing consent directives[19] from patients; consent directives framework development; consent messaging standards; architecting the consent directives management service; overriding consent directives; free form text; inter-jurisdictional access control; EHR infostructure as a messaging conduit; privacy protective EHRs locator service; data warehouses and secondary uses; record retention schedules; ensuring accuracy, correcting inaccurate information; client registry accuracy and correction; identifying the circle of care;[20] audit logging and monitoring; trusted user management and user registries; preventing exposure of EHR Client Identifiers (ECIDs); storing identifiers in domain repositories; security of EHR viewers; patient access to information in EHR infostructures; patient portals; privacy oversight collaboration; challenging compliance and breach management; and threat and risk assessments.

To each of these observations, Infoway outlined responses (for full details, see the PIA report).[21] Notable among these were: raising issues with the Privacy Forum,[22] promoting

[17] This PIA only covers privacy principles and requirements of the CSA Model Code.
[18] The majority of the observations were classed as non-technical (non-addressable by the EHR architecture) and with pan-Canadian impact. Anzen and Sextant suggested a collaborative approach to addressing them with Infoway playing a facilitating role.
[19] A consent directive is "An instruction of an individual to whom information pertains, or his/her legally authorised representative, permitting or restricting the use or disclosure of his/her information". Anzen and Sextant, op. cit., p. 10.
[20] Defined as a reference to "the individuals and activities directly related to the health care and treatment of an individual. It also covers activities related to an integrated care model, such as laboratory work and professional or case consultation with other health care providers". Anzen and Sextant, op. cit., p. 10.
[21] See pp. 62-101.

transparency in privacy and security issues, identifying solutions to apply consent directives to free-form text, extending the EHRS Blueprint to articulate how privacy and security safeguards inherent the Privacy and Security Conceptual Architecture (PSCA) would apply when the EHR Infostructure is used as a messaging conduit, removing the controversial provision for indefinite retention of data in EHRS Blueprint Version 2, identifying solutions to correct inaccurate clinical information, identifying best practices for auditing and monitoring EHR Infostructure information.

In conclusion, the PIA report recognises (p. 40) that the EHR Infostructure architecture has "few privacy shortcomings" which can be addressed through the recommendations made. It underlines the "need for a formal and appropriate due diligence process" and "for *Infoway* and jurisdictions implementing EHR Infostructures to work collaboratively to ensure that a comprehensive privacy framework to protect personal health information is in place".[23]

9.4.1 Effectiveness

The PIA report contains a lot of information (on the EHR Infostructure, privacy law, national policy initiatives, sources of information for the PIA, the evaluative framework and privacy analysis in the form of observations with responses). It graphically illustrates (p. 4) where the PIA fits into the EHR Infostructure policy development.

Using the criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	No

9.4.2 Shortcomings

Consultation with stakeholders is an important part of the PIA process. The PIA report mentions it very limitedly – i.e., the consultations conducted with jurisdictions and

[22] This is an Infoway platform set up to discuss information governance issues and solutions of EHRs. The platform has representatives from each Ministry of Health and Information and Privacy Commissioner/Ombudsmen office across the country.
[23] Anzen and Sextant, op. cit., p. 40.

stakeholders across Canada in February 2005[24] "to create a conceptual privacy and security architecture for the EHR Infostructure".[25] It does not explain who the major stakeholders in the EHR Infostructure are.

Infoway comments that it has "*contributed significantly to ensuring that the public is aware of the importance of privacy*" [italics added].[26] The contribution outlined in the PIA documents is limited to the PSCA Governance White Paper,[27] informational website material, and surveys it has commissioned on Canadian's views towards electronic health records. It is hard to gauge how significant these have been in making the public aware of the importance of privacy.

9.5 CANADA – ENHANCED DRIVER'S LICENCE PIA

Some Canadian provinces now offer an enhanced driver's licence (EDL) which is a wallet-size ID card embedded with an RFID chip.[28] The EDL has generated controversy because Canada was going to share data on the EDL with US agencies. The Privacy Commissioner of Canada and her provincial counterparts expressed concern about "pushing" (giving) Canadian databases to US government agencies (that idea was eventually dropped as a consequence of the privacy commissioners' concerns). Proponents of the EDL promoted the card as a way of speeding up the process by means of which Canadians and Americans could enter the US. The EDL was also a response to the US Western Hemisphere Travel Initiative (WHTI), which is a "legislated requirement for entry into the U.S. stemming from the 9/11 Commission and the U.S.A. Intelligence Reform and Terror Prevention Act (2004)".[29]

Along with numerous US states, several provinces have implemented their EDL programmes for Canadian citizens which include proof of citizenship to comply with the US Department of Homeland Security's Western Hemisphere Travel Initiative for entering the United States. Provinces issuing EDLs include Manitoba, Quebec, British Columbia and Ontario.

The Canada Border Services Agency (CBSA) prepared a privacy impact assessment of the enhanced driver's licence (EDL) program in January 2008.[30] The 48-page report contains an executive summary, introduction, a description of the EDL program, a data and privacy analysis, a summary table and two annexes, one of which contains a PIA questionnaire, the other references.

---

[24] See Canada Health Infoway, *Electronic Health Record (EHR) Privacy and Security Requirements Reviewed with Jurisdictions and Providers*, V1.1, Montreal, 30 November 2004, Revised 7 February 2005. https://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Requirements.pdf

[25] Anzen and Sextant, op. cit., p. 46.

[26] Anzen and Sextant, op. cit., p. 4.

[27] Canada Health Infoway, *White Paper on Information Governance in the Interoperable Electronic Health Record*, March 2007. https://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf

[28] The EDL program when "live" in April 2009. Canada Border Services Agency, "B.C's enhanced driver's licence for U.S. border use goes public", Press release, 6 Apr 2009. http://www.cbsa-asfc.gc.ca/media/release-communique/2009/2009-04-06-eng.html

[29] EDL PIA, 2009, p. 2.

[30] Canada Border Services Agency, Privacy Impact Assessment of the Enhanced Driver's Licence (EDL) Program, Ottawa, January 2008 [EDL PIA]. http://www.idforum.ischool.utoronto.ca/?q=EDL-PIA-CBSA-Jan2008

The PIA report is available on the website of the Canadian IDentity forum (the "hub for advocates campaigning against the EDLs"[31]). A Canadian Press reporter obtained the PIA following a successful Access to Information request (= a Freedom of Information request). The PIA does not appear on the CBSA website, even though it has now been released into the public domain via the journalist.

Various bits of the PIA report have been redacted out. The CBSA updated the PIA in Dec 2008, but that update seems not to be publicly available. The British Columbia PIA, dated Feb 2009, is available on the website of the Insurance Corporation of British Columbia (ICBC), a provincial Crown corporation providing auto insurance to BC motorists, driver licensing, and vehicle licensing and registration.[32]

The CBSA acts as liaison between provincial governments who are responsible for issuing drivers' licences and the American government agencies most involved in the West Hemisphere Travel Initiative.

There are some good things about this PIA, but it also has some shortcomings.

The PIA report provides on its cover page a named contact for further information, a director in the CBSA. It also provides a contact telephone number.

Canada proposed the EDL as a response to the WHTI requirements. The EDL program is voluntary. The EDL is similar to a regular driver's licence but with some additional features. Information about some of those features has been redacted out from the PIA. The PIA says (p. 2) that issuance of the RFID-equipped EDL will expedite movement of US and Canadian citizens across the border as these travellers will proceed faster through inspection lines.

The primary focus of the PIA is British Columbia's EDL Phase 1 pilot. The PIA was to be updated before Phase 2.

The PIA says the report represents a response by CBSA to requirements under the Privacy Act and Treasury Board policies, particularly the Privacy Impact Analysis Policy. It was intended to ensure that privacy considerations were adequately addressed in the collection, disclosure and reception of personal information. The PIA is based on the information and responses received following the completion of questionnaires in the PIA Guidelines.

The report says the CBSA had three meetings on the EDL program with the OPC during the summer of 2007, during which the OPC raised several issues of concern about the program. The PIA reports on those together with the CBSA's recommendations in response.

The first issue concerned the proposed EDL database containing Canadian's personal information being provided to the US Customs and Border Protection (CBP) agency and the Department of Homeland Security and the associated risks of that data being used for purposes other than travel across the US-Canada border.

[31] Parsons, Christopher, "EDL Update: Privacy Impact Assessment Released!", blog, Posted on Technology, Thoughts and Trinkets, 11 December 2008.
http://www.christopher-parsons.com/blog/technology/edl/edl-update-privacy-impact-assessment-released/
[32] http://www.icbc.com/driver-licensing/getting-licensed/edl

The CBSA says that it is developing a memorandum of understanding (MoU) with CBP that would provide "express written guidelines" on the handling of personal information and its intended usage. Under the MoU, CBSA would "seek assurances" from CBP that "appropriate auditing mechanisms are in place to safeguard the EDL information and that it will only be used for cross-border purposes". However, CBSA does not seem to have rock-hard confidence that such will actually be the case; hence, it says EDL applicants would be advised in the application form and as part of the interview process that their personal information may be disclosed to other organisations "for any purpose as authorized by U.S. law".

The decision to transmit EDL holder information to the US for Phase 1 was based on requirements and existing programs. "CBSA did not have the means to store collected EDL information nor does it currently have a need for this information."[33] CBP had a requirement for accessing stored EDL holder information, i.e., that the response time should be a maximum of half a second per query – in other words, when a border official scans the visitor's EDL, he or she should get a response from the database in less than half a second as to the card's authenticity.

The second issue raised by the OPC was the need to ensure the informed consent of participants in the BC pilot regarding the "full cycle of data collection, analysis and dissemination involving their personal information once submitted". CBSA says in response that EDL applicants would be provided with information regarding the collection, analysis and dissemination of their information on the application form and a participant's guide. EDL applicants would be advised that their personal information may be disclosed to other organisations "for any other purpose as authorized by U.S. law".

The third issue concerns the risks of the cards for fraudulent purposes, but the text of this issue has been partly redacted, so we don't know the full extent of the concern. The recommendation or response from the CBSA has been heavily redacted, but the remaining text says the EDL card will meet secure document standards.

The fourth issue raised by the OPC concerns risks posed by the collection of additional information in the EDL application process that goes beyond that required for a passport and the potential use of such information by US authorities. The recommendation (which is more of a response) from CBSA says that it and the CBP will be subject to "strict" usage guidelines as identified in the MoU. The information to be shared with the US includes the EDL holder's name, photo, date of birth, expiration date of the card, gender, citizenship, optical character recognition number unique to the EDL, the RFID tag number, issuing province and "state change reason code" (whatever that is) and height. Some other information to be shared has been redacted out of the PIA.[34] The MoU spells out that the US will conduct audits of its use of the information from Canada and share the audit results with Canada.

The fifth issue concerned the possible lack of legislated authority for CBSA to collect and retain EDL holder information (it appears that some brief text has been redacted between holder and information). The recommendation (= response) from CBSA is that it has been long-standing policy of the Canadian government to develop "enhanced commonly held documents" in response to the US WHTI requirements.

[33] EDL PIA, p. 3. The rest of this sentence has been redacted.

[34] The CBSA press release mentioned above says "The only personal information disclosed to U.S. border authorities is: first and last name, birth date, gender, citizenship, licence expiry date, your digital photograph, licence status, licence issuing province, your RFID unique identifier and tag ID number and your machine readable unique identifier."

In addition to the issues raised by the OPC, the British Columbia privacy commissioner also raised some issues with CBSA. The first was the fact that CBSA does not have a database to store EDL data and the technical challenge posed by the requirement for a response time of less than half a second to a query from a border official. The second issue was what the US would do with the personal information they get from the CBSA.

The CBSA recognises that "it is clear that any sharing of personal information encompasses inherent privacy risks". However, it developed its recommendations in the PIA report in concert with representatives of various government institutions and other entities, including the US.

In the main body of the PIA report, CBSA sets out the objectives of the PIA – to determine the privacy risks related to the EDL program, to ensure privacy concerns are identified and addressed, and to provide recommendations for mitigating the risks. It says the PIA report will be revised before the BC pilot proceeds to phase 2 – and, as mentioned above, this has happened, even though the update is not publicly available. CBSA says it consulted "partners and stakeholders" in preparing the PIAs and that the provinces would be conducting their own PIAs. It says that, in preparing this PIA, it followed the Treasury Board Secretariat's Privacy Impact Assessment Guidelines (see chapter 4 above).

The main structure of the PIA consists of three components. The first describes the EDL program, the second is a privacy analysis "which is designed to provide an assessment of compliance with privacy principles and to identify any privacy risks", and the third is a privacy risk management plan to address identified risks.

The PIA report lists the participants CBSA consulted, but all of these are government institutions and does not include the Canadian ID forum, the group lobbying against EDLs. The report does not provide any information about the nature of the consultations, how they were conducted and whether there were any iterations.

The PIA report identifies some of the information to be held on the EDL card but has redacted out other bits. It claims (p. 12) that those holding an EDL can be processed at border points two or three times faster than holders of regular documents.

The PIA includes a data flow analysis. Its privacy analysis (section 5 of the PIA report) is based on a questionnaire in the PIA Guidelines from the Treasury Board Secretariat. The core of the questionnaire are the 10 privacy principles in the PIA Guidelines which relate to accountability, collection of personal information, consent, use of personal information, disclosure and disposition of personal information, accuracy, safeguarding personal information, openness, individual's access to personal information and "challenging compliance". This last principle concerns complaint procedures consistent with legislated requirements. Following each of the questions based on the privacy principles is a relatively detailed response, which is one of the strengths of this PIA.

9.5.1 Effectiveness

This PIA report is relatively good as far as it goes. Its main shortcoming is that it does not go far enough. It is relatively detailed, well-structured and well written. It provides a good description of the project and its background. CBSA met with and consulted some stakeholders. It identified various privacy risks and made a set of recommendations for

dealing with those risks. It also foresees an updating of the PIA report, as more information became available.

Using our criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	No
identify what consultation was undertaken with which stakeholders?	No

9.5.2 Shortcomings

One obvious shortcoming is that CBSA has not posted the full PIA on its website. The full PIA has only entered the public domain because a reporter filed a FOI request. Even though CBSA redacted some bits, this PIA report shows that it is possible to make public a PIA report supposedly containing sensitive information. One cannot help wonder why CBSA couldn't make this PIA report public in any event. It is clearly in the public interest, especially given the fact that so many people have driver's licences and so many Canadians enter the US every day and that many of them may ultimately carry an enhanced driver's licence. The principal controversy raised by the EDL program was providing all of the personal information on the EDL to the US and what the US might do with all that data. These issues should be debated in the public domain, rather than behind closed government doors.

Thus, another shortcoming of the PIA is that all relevant stakeholders, including the public, were not consulted before the PIA report was finished. CBSA consulted some stakeholders but the PIA report says nothing about the nature of the consultation.

While it seems the CBSA made a good effort to identify risks – according to the 10 privacy principles – other risks might have surfaced if there had been a more open consultation and the process of finding solutions to those risks might have worked in CBSA's favour. As it was, because a reporter had to file an FOI request to get the PIA, the CBSA faced some negative press[35] and ultimately had to shelf its plan to simply give the US all of the personal data contained on every Canadian EDL. According to the press story cited in the footnote below, the Canadian government dropped plans to share the database with the US

[35] Bronskill, Jim, "Canada backpedals on sharing ID database with U.S.", The Canadian Press, Published in *The Globe and Mail*, 1 Dec 2008, last updated 31 Mar 2009.
http://www.theglobeandmail.com/news/technology/article725223.ece

government.[36] Instead, US border officials would "ping" (query) the database housed in Canada. The story says that in February 2008, the month after the PIA report was completed, federal and provincial privacy commissioners issued a joint resolution expressing concern about the EDL program's privacy and security risks, and called for safeguards including assurances the personal information of participating drivers would remain in Canada.

This PIA report in some sense highlights the importance of good privacy questionnaires. The CBSA used the Treasury Board PIA methodology and questionnaire, but it did not go beyond the questionnaire (as it might have done if there had been an open consultation with all stakeholders). Thus, one could conclude that relatively detailed questionnaires (such as that in the ICO PIA Handbook) are a good idea if assessors don't go beyond those included with the methodology they use.

Yet another shortcoming of this PIA report (and many others we have seen) is that it does not spell out for whom the PIA report is intended, how the PIA report will be used and how its recommendations will be monitored.

9.6 NEW ZEALAND – COLLECTION AND HANDLING OF BIOMETRICS AT DEPARTMENT OF LABOUR

The New Zealand Department of Labour collects and uses biometric information[37] as a "vital component of the identity establishment processes for people wishing to enter New Zealand".[38]

Biometric information collection occurs in instances such as visa applications, testing of refugees to substantiate familial relationships, border and onshore asylum, passport reading at airports and police fingerprinting. Biometric information is stored in the Immigration Application Management System (AMS), the image database (for digital photographs and scanned copies of passport biographic information), on computers attached to passport readers, the Intelligence Capability Enhancement (ICE), Refugee Quota Branch database (there is a separate database for children's information) and the immigration fingerprint database within the Police Automated Fingerprint Identification System (AFIS).

The department's internal handling of biometric information takes the following forms: use of photographs and scanned information from the image server and biographic information from AMS, photo comparisons of refugees, manual use of photos and fingerprints (via AFIS) to verify identity of asylum claimants, manual use of photos and fingerprints (via AFIS) by the Compliance and Fraud division, use of AMS data by the Immigration Profiling Group, use of

[36] The personal data of 521 BC volunteers who participated in the Phase 1 pilot was, however, sent to the US. See Parsons, op. cit., and the CBSA press release, op. cit. The press release also states that "All the information contained within the cards will be stored in a secure database located in Canada and maintained by CBSA and will only be accessed when the cardholder presents the card at the U.S. land or water border. At that point, it is used to establish the identity and citizenship of the cardholder."

[37] Section 4 of the Immigration Act 2009 specifies biometric information as being (a) any or all of (i) a photograph of all or part of the person's head and shoulders; (ii) the person's fingerprints; (iii) an iris scan; and (b) includes a record, whether physical or electronic, of any of the above things.

[38] Department of Labour, Privacy Impact Assessment: Collection and Handling of Biometrics at Department of Labour, Wellington, New Zealand, February 2011, p. 27.
http://www.immigration.govt.nz/NR/rdonlyres/AF6EC74E-F039-41DF-B477-A5B77C2DF463/0/DOL11610BiometricPIAReportFINAL.pdf (The Biometrics PIA Report)

photos by the Resolutions Team (Service Design),[39] use of facial images in ICE by Intelligence and Investigations and biometric information transfers between ICE and the photo database.

Biometric information is shared with the Five-Country Conference (FCC) partners[40] (fingerprints via the FCC Protocol and photographs where required during specific requirements) and law enforcement agencies (Police, Interpol, Security Intelligence Service, Customs, Department of Internal Affairs and Corrections).

The Department of Labour undertook a PIA to assess the Department's current and future practices with respect to the collection and handling of biometric information in accordance with section 32 of the Immigration Act 2009, which provides that the Department must complete a PIA to (a) identify the potential effects that the Act may have on personal privacy; and (b) examine how any detrimental effects on privacy might be lessened. The PIA thus sought to "identify and record the essential components of the Department's collection and handling of biometric information, both current and proposed, and to establish how the privacy risks associated with these can be managed".[41]

The PIA is in the nature of an "umbrella", providing "a framework within which ongoing assessment of the privacy implications of implementing the biometrics provisions in the 2009 Act can be addressed".[42] It was developed in a manner that would enable the integration of "subsequent implementation or project specific PIAs into a coherent document".[43]

The PIA Report,[44] dated February 2011, is 84 pages long. Its detailed contents include an introductory section on the structure of the PIA, an executive summary, summary of risks and mitigations, overview of biometric provisions in the Immigration Act 2009 and privacy governance, identification of the nature and scale of the problem, assessment of available options, scope of privacy impact assessment, analysis of guiding principles, analysis of implementation principles, risk assessment, outline of privacy enhancing responses, details of ongoing evaluation, review and monitoring. It also has various appendices that set out information on abbreviations (Appendix 1), existing privacy risk mitigations (Appendix 2), summary of implemented projects (Appendix 3) and templates for specific powers and uses of biometrics to be maintained on an ongoing basis (as mandated under section 32 (3) of the Immigration Act 2009).[45]

The sources for the topics and issues presented in the PIA report were the NZ Privacy Impact Assessment Handbook,[46] the Guiding Principles for the Use of Biometric Technologies for

[39] The team handles statutory complaints, revocations and deportations.
[40] Australia, Canada, New Zealand, the United Kingdom and the United States.
[41] The Biometrics PIA Report, p. 24.
[42] The Biometrics PIA Report, p. 7.
[43] The Biometrics PIA Report, p. 7.
[44] Op.cit., fn. 2.
[45] This provides that "the *Department* must review its privacy impact assessment if changes are made to this Act, regulations made under it, or operational policy in respect of the collection or handling of biometric information and, if the review establishes that new or increased privacy impacts have resulted from the changes, must—(a) amend or replace the privacy impact assessment; and (b) consult the Privacy Commissioner on the amended or replacement assessment.
[46] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Wellington, 2007. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf

Government Agencies,[47] the Good Practice Privacy Guidelines for the use of Biometric Technologies,[48] the Trusted Computing and Digital Rights Management Principles[49] and the Policies and Trusted Computing and Digital Rights Management Standards and Guidelines.[50]

The Department of Labour submitted the terms of reference (outlining the purpose, objective and scope, arrangements, process and deliverables of the PIA) to the NZ OPC in April 2010 and the PIA report structure was accordingly agreed. The PIA process involved both internal information gathering and external information gathering/consultation.

Internal information gathering comprised of information collection from existing documentation (i.e., policy and procedures manuals, project plans and supporting documents for proposed initiatives) and face-to-face (one-on-one or group) interviews with relevant internal personnel (discussing existing and prospective information collection and handling) in Wellington, Auckland and London. External information gathering/consultation involved discussions with external stakeholders like the Department of Internal Affairs (DIA), New Zealand Customs Service (Customs), New Zealand Police (Police), Ministry of Foreign Affairs and Trade (MFAT), New Zealand Transport Agency (NZTA), Ministry of Agriculture and Forestry (MAF), New Zealand Food Safety Authority (NZFSA) and Ministry of Justice (MoJ).

The PIA report outlines the methodology of the information gathering.[51] Depending on whether collection and handling of biometric data was current or prospective, internal interviews used either one of two indicative checklists developed by the Department of Labour. External information gathering/consultation involved a different set of interview questions. Both sets of checklists were in the nature of memory aids for interviewers rather than as scripts or questionnaires. These checklists (finalised after feedback from the NZ OPC) covered in detail the Information Privacy Principles (IPPs) of the Privacy Act 1993. There were 19 internal business units interviewed and seven external agencies (including formal agents of the department).

The report refers (p. 35) to the extensive consultation held on the Immigration Act 2009, specifically on the use of biometrics.[52] In relation to section 11 (the use of biometrics), 102 respondents[53] expressed the need for adequate safeguards and a detailed privacy impact assessment to be conducted by the Privacy Commissioner or an independent body. The respondents included businesses, community law centres, ethnic councils, government agencies, human rights groups, immigration consultants, law societies, other community groups, refugee and migrant groups, representatives of the airline and tourism industries,

[47] Cross Government Biometrics Group, *Guiding Principles for the Use of Biometric Technologies for Government Agencies*, Department of Internal Affairs, Wellington, April 2009. http://www.dia.govt.nz/pubforms.nsf/URL/GuidingPrinciplesBiometricTechnologiesBooklet.pdf/$file/GuidingPrinciplesBiometricTechnologiesBooklet.pdf

[48] Department of Internal Affairs, Good Practice Privacy Guidelines for the Use of Biometric Technologies, Wellington, September 2008.

[49] State Services Commission, *Trusted Computing and Digital Rights Management Principles and Policies*, Wellington, September 2006. http://www.e.govt.nz/library/tc-and-drm-principles-policies-sept-2006.pdf

[50] State Services Commission, *Trusted Computing and Digital Rights Management Standards and Guidelines*, Wellington, July 2007.

[51] The Biometrics PIA Report, p. 25.

[52] Department of Labour, Immigration Act Review: Summary of Submissions, November 2006. http://www.dol.govt.nz/PDFs/iar-submissions.pdf

[53] Fifty-six represented organisations and 46 individuals responded in a private capacity.

political parties, a union representative and the United Nations High Commissioner for Refugees.

The PIA identified three categories of risks: governance, handling practices and security.[54] Governance risks relate to the Department's privacy compliance framework and strategy. Handling practices risks are practical implementation issues connected to current and prospective information-handling activities. Security risks relate to storage and security aspects of biometric information. Against each risk (specified in the report), there are various mitigations recommended.[55]

The PIA report also highlights the management and technical responses of the Department to mitigate privacy risks such as privacy by design,[56] privacy-enhancing technologies (PETs),[57] and security responses and other privacy protective tools.[58]

9.6.1 Effectiveness

The best feature of the PIA is its recognition of its process as "only the first crucial step" in the implementation of biometric provisions,[59] setting up a framework for future assessments of biometrics provisions under the Immigration Act 2009. As for the PIA report itself, it aims to function as a "reference tool and see each initiative assessed separately to address specific biometric information processing functions".[60]

Using the criteria set out in section 9.1, the following results are obtained:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	Yes

9.6.2 Shortcomings

[54] The Biometrics PIA Report, p. 50.
[55] The Biometrics PIA Report, pp. 50-60.
[56] The Biometrics PIA Report, p. 61.
[57] i.e., counter privacy-intrusive technologies, anonymity PETs and pseudonymity PETs. The Biometrics PIA Report, p. 61.
[58] The Biometrics PIA Report, p. 62.
[59] The Biometrics PIA Report, p. 66.
[60] The Biometrics PIA Report, p. 7.

Though the PIA report was published and a search on the Department's website brings it up, it is not clear where it can be found on the Department's website.

The PIA report itself is not clear about when the PIA was undertaken or its duration.

Additionally, though the source material for the topics and issues of the PIA are outlined, the manner of referencing without weblinks makes finding these documents difficult (e.g., the State Services Commission's Trusted Computing and Digital Rights Management Principles and Policies).

There is lack of information about the constraints upon or limitations of the PIA.

9.7 NEW ZEALAND – GOOGLE STREET VIEW PRIVACY IMPACT ASSESSMENT

Google Street View is a Google Maps application used to explore places through 360-degree street-level imagery from public spaces and privately owned properties (that have permitted such access).[61] Google collects this imagery through its vehicles driving past locations, processes it and subsequently puts it online.

Google Street View launched in New Zealand in 2008. During the course of Street View filming in New Zealand, Google's Street View vehicles collected open Wi-Fi information[62] (easily accessible Wi-Fi information like network names) and payload information (the actual contents of communications) from unsecured Wi-Fi networks. When the revelation surfaced,[63] investigations followed. The New Zealand Privacy Commissioner formally referred this matter to the New Zealand police in June 2010.[64] On finding that there was no evidence of any criminal offence, the New Zealand police returned the matter to the Privacy Commissioner for further consideration.[65] The Privacy Commissioner conducted an inquiry and concluded that:

- Google had failed to properly notify the New Zealand public about collecting openly accessible Wi-Fi information, the collection was unfair, and
- Google had breached the Privacy Act 1993 when it collected payload information from unsecured networks without legitimate reason, and the collection was seriously intrusive.[66]

The Privacy Commissioner imposed several requirements on Google. One of the key requirements was to conduct a privacy impact assessment on "new Street View data collection activities in New Zealand", and provide a copy of the privacy impact assessment to

[61] Google Inc., Using Street View. http://maps.google.co.nz/intl/en/help/maps/streetview/learn/using-street-view.html

[62] According to the New Zealand Privacy Commissioner, open Wi-Fi information includes the device's unique identity number, a user's network name, information on whether the network is secured or unsecured and signal strength.

[63] See New Zealand Privacy Commissioner, Google and Wi-Fi Information Collection, 14 May 2010. http://privacy.org.nz/media-release-google-and-wi-fi-information-collection/

[64] New Zealand Privacy Commissioner, Google Street View: Collection of Data from Wi-Fi Networks, 10 June 2010. http://privacy.org.nz/media-release-google-street-view-collection-of-data-from-wi-fi-networks/

[65] Ogilvie, Grant, "Google Street View investigation referred back to Privacy Commissioner", Press release, New Zealand Police, 2 September 2010. https://www.police.govt.nz/news/release/25282.html

[66] New Zealand Privacy Commissioner, Google's collection of WiFi Information During Street View filming, Executive Summary, 14 December 2010, http://privacy.org.nz/google-s-collection-of-wifi-information-during-street-view-filming/

the Privacy Commissioner.[67] Google must also regularly consult with the New Zealand Privacy Commissioner about personal information collection activities.

Google Inc. published the PIA report on its website.[68] The report is 11 pages long. It contains a project description (overall aims, scope, extent and links of Street View to other projects), mapping of information flows and privacy framework, privacy impact analysis, privacy management and recommendations. Appended to the privacy impact assessment report is a report of the inspection and remediation of Google Street View Vehicles' 802.11 Wireless Network Traffic Capture Capabilities.[69]

The PIA report sets out the scope and extent of Street View in New Zealand. Google gathers imagery and vehicle positioning data with the help of cameras and equipment fixed in automobiles and trikes[70] driving on public roads and privately owned locations, where permitted.[71] After Google gathers the data, it processes and digitally publishes it. As the collected data might include images of individuals and licence plates, Google implements privacy enhancing measures such as facial and licence plate blurring and "report a problem" tool. Third parties can access the data obtained by Street View through Google's API (Application Programming Interface) feed.[72]

The PIA report outlines the information flows. The types of data collected by Street View are photographic imagery from digital camera sensors, three-dimensional laser scans and telemetry data collected from instruments such as GPS (Global Positioning System), IMU (Inertial Measurement Unit) and the vehicle's internal CAN (Controller-Area Network). This collection occurs sequentially at regularly spaced intervals. The report claims that Google, through Street View, does not intend to identify individuals with this data.[73] The data collected by Street View aims to provide "street-level views of locations in certain Google products and services".[74] Google physically transfers the data, initially written onto hard drives in the collecting vehicles, from New Zealand to the United States of America by courier, uploads it to Google servers, processes and publishes it. To maintain data security, Google holds periodic internal reviews of its data collection, storage and processing practices

[67] Other requirements include: making a statement about its Street View Wi-Fi collection activities on its official New Zealand blog (including an apology and acknowledgement of better transparency), improving privacy and information security training for all of its employees, improving review processes for its products and services and deleting payload data. These undertakings are in force for three years (from 14 December 2010).

[68] Google Inc., Google Street View New Zealand Privacy Impact Assessment, August 2011 [The Google Street View PIA Report].
http://services.google.com/fh/files/blogs/New%20Zealand%20Street%20View%20Privacy%20Impact%20Assessment%20August%202011.pdf

[69] Stroz Friedberg, LLC, carried out the inspection. Earlier, Stroz Friedberg assessed "the functionality of the source code for a Google project named 'gstumbler' and its main binary executable, 'gslite,' with particular focus on the elements of wireless network traffic that the code captured, analyzed, parsed, and/or wrote to disk". See Stroz Friedberg, Source Code Analysis of gstumbler, Report prepared for Google and Perkins Coie, 3 June 2010.
http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf

[70] Here, a reference to "tricycles outfitted to carry Street View equipment and capture imagery in areas such as hiking and biking trails". The Google Street View PIA Report, p. 1.

[71] Third party contractors (trained by Google) own these automobiles and trikes.

[72] Google specifies that there is no transfer of data as images are "controlled, hosted and served by Google". The Google Street View PIA Report, p. 2. Google's API Feed technology permits one to download any public Atom, RSS, or Media RSS feed using only JavaScript to mash up feeds with one's content and other APIs. See Google, Google Code. http://code.google.com/apis/feed/v1/

[73] The Google Street View PIA Report, p. 3.

[74] The Google Street View PIA Report, p. 3.

and physical security measures. Google follows its own code of conduct,[75] internal privacy and security guidelines and, being a member of the EU-US Safe Harbor framework,[76] partakes in annual Safe Harbor compliance certification.

The PIA report states that Google Street View's operations in New Zealand "benefited from the involvement of product counsel", "from the extensive knowledge and advice of Google's privacy law specialists and local lawyers – including external counsel with expertise in New Zealand's privacy laws such as the Privacy Act 1993…its associated principles and other potentially applicable legal frameworks".[77] It mentions a "comprehensive legal assessment focused on the determination of whether the collection of images from public spaces is prohibited under the Privacy Act". The Report also suggests that Google solicited advice on sensitive local issues such as airports and military establishments.

The privacy impact analysis in the report highlights the following privacy risks: images incidentally featuring passers-by and information such as vehicle licence plates; images triggering privacy-related sensitivities based on person-place association and images featuring sensitive locales (e.g. women's refuges).[78]

The PIA report outlines the measures taken to address privacy concerns prior to publication of images on Google Maps and Google Earth. These include:

1. training of Street View vehicle operators prior to and during collection of imagery as well as guidance on appropriate route planning;
2. disclosure to the public of collection activities (transparency about Street View's collection activities);
3. outreach and education to sensitive groups regarding the launch and flagging process[79];
4. delayed publication of images and automatic blurring of faces and licence plates prior to the posting of imagery; and
5. making available the "Report a Problem" tool (which enables members of the public to report a problem they might have with the images Google captures).[80]

The Google Privacy Assurance Program covering privacy design document reviews, training and privacy oversight complements the above-listed measures across Google's projects and products. In privacy design document reviews (applicable for launched, future and internal projects), after project leaders describe the collection and handling of user data, members of cross-functional privacy review teams[81] assess and analyse them for compliance with Google's practices and relevant laws. Google's internal audit staff may also review the privacy design documents. Google's privacy training policy includes targeted training for new employees in engineering and product management, a mandatory data security training module for all Google employees and an updated privacy component in its new employee orientation program. In October 2010, Google appointed Dr Alma Whitten as director of

[75] See Google Inc, Code of Conduct. 8 April 2009. http://investor.google.com/corporate/code-of-conduct.html
[76] See United States Department of Commerce, *US-EU Safe Harbor Framework: A Guide to Self-Certification*, United States Department of Commerce, Washington, DC, 2009.
http://digitalcommons.ilr.cornell.edu/key_workplace/645
[77] The Google Street View PIA Report, p. 4.
[78] The Google Street View PIA Report, p. 5.
[79] The flagging process refers to the process whereby Street View users flag inappropriate content or sensitive imagery for Google to review and remove.
[80] For instance, privacy concerns. The tool is available as a link at the bottom left of a Street View image.
[81] Comprising privacy and product counsel, engineers and product managers familiar with privacy matters within Google. The Google Street View PIA Report, p. 7.

privacy to oversee privacy processes, privacy by design initiatives and monitor the use of privacy practices and policies by Google employees.[82]

The Google Street View PIA report recommends that Google:[83]

- continue to improve its automatic facial and licence plate blurring technology;
- continue to fine-tune the "Report a Problem" tool based on user feedback;
- continue to improve its training program for Street View vehicle operators;
- continue to communicate with users about Street View and its collection activities;
- engage with the Office of the Privacy Commissioner regarding material changes to Street View practices outlined in the PIA, and
- continue to develop and fine-tune its Privacy Assurance Program.

9.7.1 Effectiveness

The Google Street View PIA report is concise, easy to read and publicly available. It is one of the few private company-based PIA reports in the public domain.

Using the criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	No
identify who conducted the PIA?	No
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	No
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	No

9.7.2 Shortcomings

The Google Street View PIA is not of the nature envisaged by the New Zealand Privacy Commissioner in its PIA Handbook as a "tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers",[84] rather it was the result of obligation imposed upon Google by the New Zealand Privacy Commissioner as a result of the inquiry launched into Street View's unauthorised collection of Wi-Fi information. In this sense, this PIA is an example of "retrofit".[85]

[82] The Google Street View PIA Report, p. 8.
[83] The Google Street View PIA Report, p. 8.
[84] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook,* Auckland/Wellington, 2007. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf
[85] Ibid.

The PIA report is a bare bones minimum. It leaves out several vital details. It does not identify who conducted the PIA or name the author(s) of the PIA report. Neither does it provide information on the duration of the PIA, nor does it outline the assumptions underlying the assessment or the terms of reference.

The description of information flows does not provide diagrams illustrating the flows of personal information (recall how the New Zealand PIA Handbook recommends that flow charts clearly depict the manner of data collection, internal circulation and dissemination beyond the organisation).[86]

The PIA report mentions a "comprehensive legal assessment".[87] However, the report does not explain how Google Street View complies specifically with relevant legislation, particularly the Information Privacy Principles (IPPs) of the Privacy Act 1993. The Report states that Google transfers Street View data outside New Zealand, yet does not (as the NZ PIA Handbook recommends) recognise any special sensitivities in this respect.

The PIA Report also offers no details of the consultations held with stakeholders – particularly those most affected by the implementation of Street View's collection and use of their personal information.

There is also no mention of the involvement of the New Zealand Privacy Commissioner in the PIA process, though the report mentions in its recommendations that Google will "engage with the Office of the Privacy Commissioner regarding material changes to Street View practices outlined in this PIA".[88]

9.8 UK – INTER-AGENCY COMMUNICATION TOOL (IACT)

eCare is the Scottish Government's, multi-agency, information-sharing framework covering, inter alia, consent, standards, security, procurement, organisational development and technical issues relating to the electronic sharing of personal data. It is delivered through a network of 14 data sharing partnerships (DSPs)[89] across Scotland. Each partnership has an eCare Multi-Agency Store (MAS) database,[90] hosted in the Atos Origin data centre in Livingston. The eCare programme has the following responsibilities:[91]

- to implement a framework which enables secure sharing of sensitive personal information;
- to make available to local partners the capability for Child protection Messaging (CPM) and Single Shared Assessment (SSA,) and to allow local partners to use the infrastructure for similar agreed functions;

[86] Op.cit., fn. 24.
[87] The Google Street View PIA Report, p. 4.
[88] The Google Street View PIA Report, p. 8.
[89] A data sharing partnership refers to a group of local agencies sharing data via a single Multi-Agency Store (MAS) and sharing in its governance. DSP areas are currently coterminous with the 14 Health Board areas.
[90] A MAS is a data repository hosted in the Atos Origin Managed Technical Service (MTS) and accessed via secure local government and NHS networks. Local agencies connect to MAS data through their existing business application, using local software adapters. There are 14 eCare MASs.
[91] The Scottish Government, eCare/GIRFEC inter-Agency Communication Tool (iACT) Privacy Impact Assessment, Version 1, 17 November 2010.
http://www.scotland.gov.uk/Topics/Government/PublicServiceReform/efficientgovernment/DataStandardsAndeCare/pia, p. 13 (the eCare/GIRFEC iACT PIA Report).

- to support policies on SSA, Getting it right and Early Years, in line with government commitments made in those policy areas;
- to explore the scope for wider use of eCare, as directed by the eCare Programme Board, for individuals who require multi-agency intervention.

The Scottish government's eCare inter-agency communication tool, called iACT, aims to "provide practitioners with general electronic support to the day-to-day exchanges of case-related information that are necessary for better inter-agency collaboration within Scottish children's services while also respecting the privacy of children and their families".[92] The inter-agency communication system supports the government's objectives of early intervention and improved services for children and families as part of its "Getting It Right For Every Child" (GIRFEC) policy. The government designed the system to help users communicate securely and safely with other users or services with interests in children and to share data appropriately.

The Scottish Government undertook a privacy impact assessment of the eCare iACT application "which enhances the existing eCare data sharing Framework with targeted messaging capabilities, to support the data sharing requirements of the Getting It Right For Every Child (GIRFEC) policy".[93] The eCare/GIRFEC PIA report outlines the results. The second iteration of the PIA report, referenced here, follows the guidelines contained in the 2009 PIA Handbook produced by the UK Information Commissioner's Office (ICO).[94]

The PIA report is 116 pages long. Its contents include: purpose, objectives and rationale of the PIA, privacy and Scottish Government privacy approach, detailed overview of GIRFEC and eCare iACT, privacy analysis (data sharing, stakeholder privacy concerns, information analysis and privacy risks and issues), privacy features, controls and mitigation and recommendations. Its appendices provide additional details on the PIA approach (Appendix A), key stakeholders and PIA engagement activity (Appendix B), initial privacy risk log (Appendix F), system privacy features detail (Appendix G), responses to consultation and engagement (Appendix H) and mapping of design features to Scottish Government privacy principles (Appendix I).

The eCare/GIRFEC iACT PIA report follows the ICO Handbook's five-stage approach.[95] In the *preliminary* stage, after carrying out an evaluation based on initial project documentation and stakeholder analysis, the internal eCare iACT team determined the need for a full-scale PIA. In the *preparation stage,* the team established a privacy consultative group (PCG), the PCG's terms of reference and an initial consultation strategy. The team conducted an initial stakeholder analysis and identified privacy principles to guide the risk assessment and system design. The *consultation and analysis* stage included an initial PIA analysis[96] (which resulted in a revision of the high-level architecture and production of a system demonstration tool[97]), revision and planning and a second PIA phase with wider consultation. The *documentation*

[92] The eCare/GIRFEC iACT PIA Report, p. 14.
[93] The eCare/GIRFEC iACT PIA Report, p. 5.
[94] The first iteration, based on the 2007 ICO Handbook, was a "technically focussed document". The second iteration included more about communication and engagement with stakeholders.
[95] ICO Handbook, 2009.
[96] This consisted of internal PIA workshops, mapping of information flows, risk identification and assessment and the initial PIA report. The government conducted the initial PIA between December 2008 and July 2009.
[97] The PIA team used the demonstration tool in workshops focused on practitioner system requirements and privacy. After the workshops, the Scottish Government revised the system architecture and PIA documentation to feed into the requirements and design phase of eCare/IACT. The eCare/GIRFEC iACT PIA Report, p. 50.

stage involved consultation with the PCG, a re-drafting of the PIA report and updating of the risk and issue documentation for publication and dissemination. The *review and audit* involved and envisages, on an ongoing basis, reviewing and auditing the technical and governance systems against the PIA report and risk management, recommendations and compliance assessment.[98]

9.8.1 Effectiveness

The eCare/GIRFEC iACT PIA report is a good example not only of the way the PIA process is supposed to be conducted as outlined in the ICO's PIA Handbook, but also of the ICO's recommendation that organisations meet and exceed legal requirements through PIAs.[99] In addition to checking for compliance with the Data Protection Act 1998, the PIA used the Scottish government's identity management and privacy principles[100] as a benchmark for analysis. More importantly, the PIA report comprehensively maps out the project's privacy risks and identifies ways of mitigating those risks.[101]
There are other positive features of the PIA report. In addition to being relatively thorough and precise, the report outlines its scope and limitations.[102] Stakeholder engagement and stakeholder consultation in the PIA process is another strong feature.[103] The report underlines the importance of a PIA as a "cyclical process".[104]

Using our criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	Yes

9.8.2 Shortcomings

[98] Appendix A, The eCare/GIRFEC iACT PIA Report, pp. 48-50.
[99] ICO Handbook, 2009.
[100] The Scottish Government, Draft Identity Management and Privacy Principles, August 2009. http://www.scotland.gov.uk/Resource/Doc/82980/0085087.pdf; The Scottish Government, Identity Management and Privacy Principles: Privacy and Public Confidence in Scottish Public Services, Version 1.1, May 2011 (current version). http://www.scotland.gov.uk/Resource/Doc/82980/0116729.pdf
[101] Appendix F, eCare/GIRFEC iACT PIA Report, pp. 61-81.
[102] The eCare/GIRFEC iACT PIA Report, p. 10.
[103] The eCare/GIRFEC iACT PIA Report, Appendix B (Key Stakeholders and PIA engagement activity), p. 51; Appendix H (Responses to consultation and engagement), p. 90.
[104] The eCare/GIRFEC iACT PIA Report, p. 5.

On the negative side, though the eCare/GIRFEC iACT PIA report is a good model of the UK ICO PIA framework, and published on the eCare Programme website,[105] it has not been publicised as such, particularly beyond Scotland[106] so that lessons could be learnt from its experience. The report itself also acknowledges that one of its key limitations was the lack of direct engagement with children, who are data subjects in the eCare/GIRFEC iACT system, due to resource constraints in the PIA process.[107]

9.9 UK - CHILD SEX OFFENDERS DISCLOSURE SCHEME

The UK government introduced the Child Sex Offenders Disclosure Scheme (the CSO Disclosure Scheme or Sarah's Law) following publication of the Review of the Protection of Children from Sex Offenders.[108] Sarah's Law derives its name from Sarah Payne, an eight-year old girl who was abducted and murdered by a previously convicted child sex offender in July 2000. After her murder, a media campaign sought to introduce Sarah's Law – a UK version of the US-based Megan's Law. Megan's Law derives its name from seven-year old Megan Kanka who was killed by a convicted sex offender who had moved into her New Jersey neighbourhood. Megan's parents campaigned for the right for parents to know about sex offenders in their neighbourhoods. Subsequently, the New Jersey legislature passed Megan's Law requiring convicted sex offenders to register with the authorities and enabling people to find out whether registered offenders live in their neighbourhoods.[109] All states in the US have implemented some form of Megan's Law.[110] Sarah's Law differs from Megan's Law.[111] Sarah's Law provides strict controlled access to information about offenders; Megan's Law permits direct uncontrolled public access to information about offenders.[112]

The CSO Disclosure Scheme is a tool in the Multi-Agency Public Protection Arrangements (MAPPA) process[113] for managing sexual offenders in England and Wales.[114] It permits

[105] See Scottish Government, iACT Privacy Impact Assessment, 23 December 2010. http://www.scotland.gov.uk/Topics/Government/PublicServiceReform/efficientgovernment/DataStandardsAndeCare/pia

[106] The Scottish Government has drawn attention to the PIA. See: The Scottish Government, Draft Identity Management and Privacy Principles: Privacy and Public Confidence in Scottish Public Services, Scottish Government Response to the Public Consultation, 23 December 2010. http://www.scotland.gov.uk/Resource/Doc/16999/0110003.pdf

[107] The eCare/GIRFEC iACT PIA Report, p. 10. The Report states, "This is being taken forward by the eCare and GIRFEC programmes and will be addressed in the Recommendations in GIRFEC and the eCare iACT project."

[108] Home Office, Review of the Protection of Children from Sex Offenders, June 2007. http://webarchive.nationalarchives.gov.uk/20100413151441/http:/www.homeoffice.gov.uk/documents/CSOR/child-sex-offender-review-1306072835.pdf?view=Binary

[109] Registration and Notification of Release of Certain Offenders Act, N.J. Stat. Ann. §§2C:7-1 (1995).

[110] In 1996, a federal amendment was made to the *Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act* 42 U.S.C. 14071(a) (3) requiring all states to establish community notification systems relating to sex offenders. States thus have websites permitting people to search for sex offenders living in the area.

[111] For a more detailed comparison, see Griffin, Lissa and Kate Blacker, "Megan's Law and Sarah's Law: A Comparative Study of Sex Offender Community Notification Schemes in the United States and the United Kingdom", 46 *Criminal Law Bulletin*. Vol. 46, No. 6, 2010, pp. 987-1008.

[112] This information includes names, addresses and photographs.

[113] National MAPPA Team, MAPPA Guidance, National Offender Management Service Public Protection Unit, Version 3.0, 2009.
http://www.justice.gov.uk/downloads/guidance/prison-probation-and-rehabilitation/public%20protection%20manual/10004894MAPPAGuidance_2009_Version3.pdf

parents, guardians and carers of children to register their interest in protection their child against a convicted sex offender. When an individual is convicted of a child sex offence[115], the named individual is considered a risk. If authorities think there is risk of harm to the child, they will disclose information about the offender to the parents, guardians and/or carers.

Authorities piloted the CSO Disclosure Scheme in Cambridgeshire, Cleveland, Hampshire and Warwickshire for 12 months from September 2008, then rolled it out nationally on a phased basis. The scheme now is available across all 43 police forces in England and Wales. It introduces a "more formal mechanism for a person to make an application for information about a particular individual who has contact with a child or children, therefore alerting the authorities to contact an offender may be having with a child which they may not previously have been aware of".[116] This scheme does not enable the automatic disclosure of child sex offender details to the public.

Working of the scheme

The scheme is a disclosure and risk management system that involves the identification of convictions (including cautions, reprimands and final warnings) for child sexual offences. The process, envisaged as a broad one, must be "utilised for gaining information about *any* person who poses a risk of harm to children".[117] An application under this scheme must concern a child or children who may be at risk of serious harm from named or identified subjects. The example cited is as follows: A new person has moved into the child's life and the applicant would like to ensure that the subject does not have a known history of offending such that they would pose a risk of serious harm to children.[118] The application does not need submission of evidence of concern in its support. However, all cases must follow the procedures outlined in the CSO Guidance.

The scheme process involves several stages, as outlined below.[119]

The first stage is *Initial Contact with the Police (Registration of Interest).* This involves the applicant's initial contact with the police reporting concerns. The applicant can make contact at a police station, in an encounter with street police, during an incident call, telephone call or online reporting, if available. The police are to conduct an initial risk assessment at this stage to establish if any urgent action is required in cases of imminent risk of harm to a child or other person.

The second stage is *Face to Face Contact.* Here the police meet applicant to confirm that the request is genuine (not malicious), to establish further details to assess risk. The scheme recommends a revisitation of the first stage risk assessment and filling in any information gaps.

---

[114] Home Office, The Child Sex Offender (CSO) Disclosure Scheme Guidance Document, 29 October 2010. http://www.homeoffice.gov.uk/publications/crime/disclosure-scheme-guidance/disclosure-scheme-guidance?view=Binary (CSO Scheme Guidance Document)

[115] "Child sexual offences" are defined as offences listed in Schedule 34A of the Criminal Justice Act 2003. See Appendix G, CSO Guidance Document for a copy of this schedule.

[116] Home Office, Report of a Privacy Impact Assessment conducted by the Home Office in relation to the Child Sex Offenders Disclosure Scheme, Autumn 2010. http://www.homeoffice.gov.uk/publications/crime/disclosure-scheme-guidance/privacy-impact-assessment?view=Binary (CSO Disclosure Scheme PIA Report)

[117] CSO Disclosure Scheme Guidance Document.

[118] CSO Disclosure Scheme Guidance Document.

[119] For full details of the process, see the CSO Scheme Guidance Document.

The third stage is *Empowerment/Education.* Police give the applicant an information pack about the disclosure scheme which includes measures that can be taken to safeguard their children's welfare.

The fourth stage is a *Full Risk Assessment.* The scheme has a list of questions to help police assess risk. The police are also expected to review the information received in the initial contact and face-to-face stages and check any relevant information held in the Police National Computer (PNC),[120] ViSOR,[121] force local intelligence systems and the IMPACT Nominal Index (INI)[122] databases.

The fifth stage is *Decision Route "Concerns" or "No Concerns".* At this stage, the police must decide whether the applicant has legitimate concerns. The applicant has legitimate concerns, if the police find that the individual identified by the applicant has convictions for child sexual offences or other convictions relevant to safeguarding children.

The sixth stage is *Disclosure and Non-Disclosure.* The CSO scheme provides two options: non-disclosure in cases where the police find the applicant's concerns are not legitimate or disclosure of information to the applicant where they find the concerns are justified. For non-disclosure in case of "no concerns", Appendix E of the Guidance provides a template letter with the recommended form of wording.[123] Similarly, in case of disclosure, Appendix F contains a disclosure form setting out the minimum standard of information to record.[124] The police read the form through with the applicant, get it signed and retain it following disclosure. Since information about a person's convictions is regarded as sensitive personal data,[125] the police must ensure that the disclosure accords with the eight data protection principles in the Data Protection Act 1998.[126]

In 2010, the Safeguarding and Public Protection Unit of the Home Office conducted a small-scale PIA[127] on the CSO disclosure scheme taking into account pilots in Cambridgeshire, Cleveland, Hampshire and Warwickshire. In conducting the PIA, the Home Office consulted the ICO's Handbook and used other PIAs conducted within the Home Office as models.

The PIA team advanced several reasons for conducting a small-scale PIA: first, the project did not involve the introduction of new legislation or policy. Second, the police expected to collect, use and disclose information in specific circumstances following a risk assessment. Third, the PIA team argued that police expected to disclose information on a case-by-case basis, based on each application's risk assessment rather than bulk data exchange. The PIA report states, "The project had privacy issues associated with it, but not the large inherent

[120] The primary national police computer system in the UK, available to the police and other criminal justice agencies. It contains comprehensive details of people, vehicles, crimes and property.
[121] A national database used by Public Protection Units to manage offenders with sex offender registration conditions imposed on them following criminal convictions and information on violent and potentially dangerous people.
[122] A computer system that permits officers to find out relevant information, on persons under investigation, from other police forces.
[123] CSO Disclosure Scheme Guidance Document, Appendix E.
[124] CSO Disclosure Scheme Guidance Document, Appendix F.
[125] See s 2 (g), Data Protection Act 1998.
[126] CSO Disclosure Scheme Guidance Document, p. 15. The CSO Disclosure Scheme Guidance Document, Appendix H provides details of these principles and guidance on their application. See Appendix H, The Data Protection Act 1998. http://www.homeoffice.gov.uk/publications/crime/disclosure-scheme-guidance/appendix-h?view=Binary
[127] CSO Disclosure Scheme PIA Report.

risks that would warrant a full scale PIA, for example those typically associated with new policy areas, major new databases, or using data collected in connection with one purpose for very different purposes."[128]

The Home Office published the 18-page PIA report on its website.[129] The report was intended to be "time and cost effective". Its contents include an overview, outline and practical arrangements of the scheme, purpose of the report and legal basis for disclosure. It also contains information on the PIA with regard to awareness, scoping, impacts, privacy risks and mitigation.

9.9.1 Effectiveness

In terms of effectiveness, the CSO PIA report, as intended by the Home Office, is easy to read and gives "enough background to be read alone" in terms of the disclosure process. It is easily accessible on the Web through Google search and features in the publications section of the Home Office website alongside the CSO Disclosure Scheme Guidance.[130]

The PIA report highlights privacy issues and risks in relation to the scheme: inappropriate disclosures, further disclosures of information with good or malicious intent, disclosures resulting in acts of vigilantism (harassment, criminal damage, violence) and failure of registered sex offenders (RSOs) to comply with their notifications/registration requirements. The report outlines measures for minimising negative privacy impacts: face-to-face briefings with RSOs prior to the scheme's going live; maintaining the specificity of disclosure; steps to ensure information is not further disclosed and that information is only used to keep children safe; reminders that breach of confidentiality agreements would constitute a breach of the DPA 1998 and invoke legal proceedings.

Using the criteria set out in section 9.1, the following results are obtained:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	No[131]
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	No
get published on the organisation's website? Is it easily found there? If the PIA	Yes

[128] See CSO Disclosure Scheme PIA Report.
[129] Home Office, Report of a Privacy Impact Assessment conducted by the Home Office in relation to the Child Sex Offenders Disclosure Scheme, Autumn 2010. http://www.homeoffice.gov.uk/publications/crime/disclosure-scheme-guidance/privacy-impact-assessment?view=Binary
[130] CSO Disclosure Scheme Guidance.
[131] The report is vague about this. It states that there has been "a project board running from the early creation of the pilot up to the current date. There are various members of other agencies that sit on this project and have had opportunity to comment on privacy issues arising along the way both with regard to the actual mechanisms of the process and the creation of the national guidance."

report was not published (even in a redacted form), was there an explanation as to why it has not been published?	
identify what consultation was undertaken with which stakeholders?	No[132]

9.9.2 Shortcomings

This PIA report falls short in the following respects: First, the report, when read alone, is not clear about when the PIA was conducted. It is thus problematic for an external observer to determine whether the PIA had an opportunity to influence the design or principles underlying the CSO disclosure scheme. Second, the PIA report itself mentions, but fails to identify stakeholders and the specific nature of the consultations carried out.[133] Thus, it is not clear whether stakeholders, as the ICO recommends, have had an opportunity to "have their perspectives reflected in the project design".[134]

The report also does not make any recommendations. In terms of follow-up, it states that the Home Office would "closely monitor and review the Scheme's operation" in consultation with partners,[135] through ongoing review of the privacy impacts, and monitoring compliance with the specific privacy and security arrangements.[136] On enquiry, the Home Office clarified that the PIA is "being kept under review but has not been amended since publication".[137]

9.10 US – DHS PIA OF FUSION CENTERS

The DHS Fusion Center PIA is a comprehensive, 42-page document. The PIA was produced pursuant to Section 511 of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Homeland Security Act of 2002 and in consideration of the Privacy Act of 1974.[138] The 9/11 Commission Act also requires the DHS to undertake a concept of operations report for the fusion centre initiative which includes a civil liberties impact assessment as well as a PIA. The document, dated 11 December 2008, is available on the DHS website, although it is fairly difficult to locate by browsing.

[132] In respect of stakeholders, the report states, "The process being assessed has already worked successfully in pilot and provided information that would have been gathered as part of any stakeholder engagement." (See 2.4). For a report of the pilot, see Kemshall, Hazel, and Jason Wood et al., *Home Office Research Report 32 - Child Sex Offender Review (CSOR) Public Disclosure Pilots: A Process Evaluation*, London, 3 March 2010. http://webarchive.nationalarchives.gov.uk/20100503160445/rds.homeoffice.gov.uk/rds/pdfs10/horr32c.pdf

[133] Here, it refers back to the stakeholder engagement during the pilot of the scheme. These were 11 purposively selected national stakeholders and 21 selected local stakeholders, including probation public protection leads. See Kemshall and Wood, op. cit., 2010, p. 2. It is not evident how the stakeholder engagement during the pilot concerned or addressed privacy impacts. The pilot evaluation is also difficult to find unless one knows what one is looking for. On enquiry, the Home Office clarified that "There was consultation through the Project Board which oversees the implantation of the Scheme, this includes central Government Departments, the police, the National Police Improvement Agency (NPIA), The Child Exploitation and Online Protection Centre (CEOP), Barnardos, NSPCC and the Lucy Faithfull Foundation." E-mail communication from Ms Victoria Presland, Safeguarding Policy Advisor, Safeguarding and Public Protection Unit, Home Office, 20 July 2011.

[134] ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

[135] Unspecified in the CSO Disclosure Scheme PIA Report Report.

[136] CSO Disclosure Scheme PIA Report, 2.5.

[137] E-mail communication from Ms. Victoria Presland, Safeguarding Policy Advisor, Safeguarding and Public Protection Unit, Home Office. 20 July 2011.

[138] Department of Homeland Security, Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, 11 Dec 2008, p. 1.

The document includes a four-page executive summary and a table of contents followed by an abstract, introduction and several chapters, including chapters on DHS Privacy Office Interaction with Fusion Centers, Fair Information Practice Principles, Fusion Centers and Privacy Concerns, a Privacy Office Follow-up and Conclusions. There is also a list of Responsible Officials, an Approval Signature Page and an Appendix of Authorities and Materials. The Appendix lists a number of fusion centre manuals, information-sharing guidelines and a civil liberties policy document.

The PIA states that it was performed internally by the Director of the State and Local Program Managers Office and reviewed by the Chief Privacy Officer of the DHS. Although detailed information about the methodology used to conduct the PIA is not provided, the PIA has utilised stakeholder engagement techniques and is intended to be a living document. The PIA states that the Privacy Office used published reports authored by the government and privacy advocacy community to outline and understand privacy concerns surrounding the fusion centre model. Privacy officials also "toured fusion centres around the country, participated in conferences, met with representatives from the privacy community and met with representatives from the privacy advocacy community, and held a public meeting of the DPIAC [Data Privacy and Integrity Advisory Committee] to hear testimony about privacy issues".[139] Participants in the public meeting included the Electronic Privacy Information Center (EPIC), The Constitution Project, and The American Civil Liberties Union (ACLU), and the PIA report states that individual fusion centres also held meetings with local privacy advocates. The DHS argues that further information exchanges will "assist the public in understanding the mission and practices" of the fusion centres and that centres should continue this interaction to increase understanding and transparency within communities".[140]

The PIA is also a living document which will be reviewed and revised as fusion centres mature. Specifically, the US Congress mandated that the DHS issue a report on privacy in relation to the fusion centres one year after the program was implemented.

The fusion center initiative

The fusion centre initiative is intended to enable bi-directional information sharing between the DHS and state, local and regional fusion centres. Fusion centres are defined in the amended Homeland Security Act as "a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity".[141] In order to facilitate this, the DHS has assigned trained intelligence analysts to the fusion centres provided that those centres meet certain criteria, including having adequate privacy provisions. DHS analysts assigned to fusion centres assist law enforcement agencies and other emergency response providers to develop an accurate threat picture, review homeland security information, create intelligence products derived from information and assist in the two-way dissemination of such intelligence products. However, the federal government cannot set policy for local fusion centres as they fall under state or local jurisdictions, but the DHS can make recommendations, and the PIA focuses on efforts by the DHS to encourage fusion centres to include privacy protections in their operations. Furthermore, the PIA is limited to the privacy implications of fusion centres' use of personally identifiable information (PII). While the DHS acknowledges that this

[139] Ibid., p. 25.
[140] Ibid., pp. 14-15.
[141] Quoted in ibid., p. 4.

limiting in scope will not address all privacy issues introduced by fusion centres, it suggests that further privacy issues are best addressed by individual states in a form similar to a PIA.

The nature of personal information used

According to the PIA report, fusion centres analyse "pieces of raw, unanalyzed data that identifies persons, evidence, events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event [including] criminal histories and driving records; statements by witnesses, informants, and suspects; vehicle registration information; banking and other financial information; and police reports".[142] Citron and Henry note that information such as "property records, immigration records, public health data, car rentals, postal services, utility bills, insurance claims and suspicious activity reports" may also be included.[143] However, the PIA report notes that even when raw data contains PII, federal agents must delete or anonymise the PII if the recipient is not authorised to receive it, or if they do not need to know it.

Privacy issues/risks identified

The PIA identifies seven specific risks to privacy regarding the use of personal information by federal agents in fusion centres and briefly describes resolutions to these risks, including:
1. Justification for fusion centres, where the public may not understand how their information could be used. This can be mitigated via transparency principles such as regular and aggressive public accounting of fusion centre activities which can increase public support.
2. Ambiguous lines of authority, rules and oversight, where state and local employees are responsible for adhering to their own state laws while federal employees must adhere to federal laws. Training will mitigate this concern, particularly through principles of purpose specification and use limitation. Centres must also draft their own privacy policies that are at least as good as the DHS policy and comply with it.
3. Participation of the military and private sector, where the DHS argues that concern about military participation is beyond the scope of the PIA; however, each fusion centre should review this PIA and prepare its own documentation. Concerns around private sector participation can be mitigated by restricting the sharing of PII with the private sector.
4. Data mining, where the PIA acknowledges that data mining may raise privacy concerns. The Privacy Office will consider this issue when it updates the PIA.
5. Excessive secrecy, where the PIA recommends that a written privacy policy will force fusion centres to document their legal authority to undertake activities, and "will significantly reduce the likelihood that centers will use their powers inconsistent with their authorities".[144]
6. Inaccurate or incomplete information, where the privacy office understands that wide information sharing will increase the possibility that incorrect or incomplete information can negatively affect individuals. The DHS recommends that fusion centres establish an accuracy policy and provide error notice to privacy officials. Furthermore, redress procedures will mitigate the extent of the impact of such incorrect or inaccurate information.
7. Mission creep, where fusion centres have already expanded beyond their first mission and centres are encouraged to describe their own legal authorities and privacy compliance processes in their foundational documents.

[142] Ibid., p. 7.
[143] Citron, Danielle Keats, and Leslie Meltzer Henry, "Visionary Pragmatism and the Value of Privacy in the Twenty-First Century", *Michigan Law Review*, Vol. 108, No. 6, April 2010, p. 1116.
http://www.michiganlawreview.org/articles/visionary-pragmatism-and-the-value-of-privacy-in-the-twenty-first-century
[144] DHS, 2008, p. 28.

General resolutions identified

In addition to these specific risks and resolutions, the PIA also notes that there are processes and polices that mitigate privacy risks in general. These include both training and privacy guidelinesr policies for fusion centres. Throughout the PIA, the DHS asserts that appropriate training will support the privacy policies of the DHS and the fusion centres. Alongside training, fusion centres should take account of different guidelines and privacy policies, including Fusion Center Guidelines published by the DHS and the Department of Justice, Information Sharing Environment privacy guidelines and Fair Information Practice Principles. Fusion centre guidelines ensure that fusion centres develop, publish and adhere to privacy and civil liberties policies consistent with federal, state and local laws as well as ensure that data security measures are in place.[145] Specifically guideline 3 "urges" fusion centres to include a privacy committee in its governance structure and fusion centre governing bodies should liaise with the DHS privacy office in deciding upon their operating procedures. Guideline 8 also includes a list of specific elements that a privacy policy should include (although the list is too extensive to reproduce here) and states that fusion centres should provide a mechanism to ensure that the privacy policy is adhered to. Furthermore, under the Information Sharing Environment, state, local and tribal agencies must meet minimum requirements that their privacy policies are "at least as comprehensive" as requirements applicable to federal agencies.[146]

In addition to these policy documents, the PIA report states that FIPPs developed in the Privacy Act of 1974 should be implemented, including transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing. To increase transparency, the PIA report states that fusion centres should make their written privacy policies and PIAs available to the public and engage with local privacy advocacy communities.

The DHS makes recommendations for specific issues such as redress, data quality and information security. Regarding redress, the PIA report states that although in intelligence and law enforcement settings full and open redress is not always possible, fusion centres should establish mechanisms to track and handle privacy complaints and concerns. In relation to data quality, the PIA report states that fusion centres are prohibited from collecting and maintaining information on criminal intelligence systems unless it is relevant to criminal conduct or activity. Furthermore, operators "must periodically review information and delete that which is misleading, obsolete or unreliable" and inform other agencies that the information has been deleted. The document states that data relevance is further ensured by requiring that information be deleted after five years. Finally, regarding information security, the PIA report recommends that overlapping steps be taken to prevent unauthorised use and that a sanction policy to ensure compliance with privacy policies be established.

9.10.1 Effectiveness

This PIA report is relatively effective and offers a fairly comprehensive discussion of applicable laws and policies and the privacy risks and resolutions utilised by the fusion centre programme. Using our criteria set out in section 9.1 above yields the following results:

Did the PIA report	

[145] DHS, 2008, p. 6.
[146] DHS, 2008, p. 13.

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	No
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	Yes
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	Yes

One of the key strengths of the document is that it is intended to be a living document, and the DHS expects it to undergo revisions as systems are changed, as fusion centres themselves mature and as new privacy risks or resolutions are identified. The document has also been published and prepared after consultation with different types of stakeholders including external stakeholders and privacy experts. This public consultation is set to continue with the DHS encouraging local fusion centres to continue consulting local privacy advocates. This will assist fusion centres and the DHS in identifying privacy issues early and altering programmes as necessary.

9.10.2 Shortcomings

Despite these strengths, this PIA report has shortcomings. It does not spell out exactly what information is collected from individuals, how this information is shared with other agencies, how long it is retained and what mechanisms are in place to ensure its accuracy. The DHS recommends appropriate staff training and comprehensive privacy policies in order to spell out some of these issues, but more specific information would assist in mitigating privacy risks and further increase transparency.

Another key shortcoming is the lack of specificity in relation to both the privacy risks and the potential solutions. For example, the PIA report states that fusion centres should establish their own privacy policies, but the exact content of these privacy policies is left open to interpretation. Furthermore, the report argues that fusion centres create risks such as data mining and inaccurate information, but does not state what the specific risks are for individuals. In contrast, Citron and Henry state that because fusion centres also flag persons of interest, individuals could be incorrectly labelled as criminals or terrorists.[147] They note that fusion centres may disclose information in ways which infringe upon or compromise privacy. Based on information from fusion centres, people could lose their jobs, be denied a loan or experience other unfair treatment.[148]

[147] Citron and Henry, 2010.
[148] Ibid.

9.11 US – PRIVACY IMPACT ASSESSMENT UPDATE FOR THE US-VISIT PROGRAM

The Department of Homeland Security (DHS) privacy impact assessment for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) programme is 42 pages long and was performed internally by the US-VISIT privacy officer. After review by the DHS Chief Privacy Officer, the document, dated 1 July 2005, was published on the DHS website.[149] The PIA states that it was undertaken in accordance with the Office of Management and Budget (OMB) guidance of 26 Sept 2003 for implementing the E-Government Act of 2002. The PIA was initially performed for the implementation of the US-VISIT programme, and it has been updated as necessary to reflect changes to the programme. The PIA document begins with a short overview followed by eight sections and five appendices. The eight sections consist of a description of the different increments for implementing the full US-VISIT programme; a system overview section that explains what data is being collected and why; a system architecture section that explains the structure of the system; an administrative controls and access to data section, explaining who has access and how this access is managed; an information lifecycle and privacy impacts section, outlining these issues for different increments; a section that outlines design choices for the different increments; and finally a summary and conclusions section. The five appendices include a list of references, a list of acronyms, details of data flows, details of security safeguards for privacy protection and details of privacy threats and mitigations.

While there is no specific information surrounding the methodology that the PIA utilised, the different updates to the PIA report suggest that the PIA for the US-VISIT programme was intended to be a living document. Specifically, it has been updated regularly due to changes and improvements in the technologies and systems implemented. The first US-VISIT PIA was published on 4 Jan 2004 at the initial deployment of the US-VISIT programme and time pressures meant that no external consultation took place, nor was the programme substantially changed as a result of the publication of the PIA. However, after this initial publication, the Chief Privacy Officer (CPO) hosted a consultation activity with privacy advocates and immigration groups who were invited to express concerns about issues such as a lack of information on redress and unclear rules on data quality and data retention.[150] According to Dempsey, the CPO promised that these issues would be addressed. Furthermore, as part of its privacy awareness programme, the PIA report states that the US-VISIT programme has its own privacy officer and that extensive stakeholder outreach and dissemination activities have taken place and will continue to take place as the programme expands.

The US-VISIT project

According to the PIA report, the purpose of the US-VISIT project is to "implement an integrated entry and exit data system to record the entry into and exit out of the United States of covered individuals; verify identity; and confirm compliance with the terms of admission to the United States".[151] The implementation of the US-VISIT project has taken place

[149] Department of Homeland Security, *Privacy Impact Assessment Update for the US-VISIT Program In Conjunction with the Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Ports of Entry*, 1 July 2005. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisitupd1.pdf

[150] Dempsey, James X., Statement before the House Committee on the Judiciary Subcommittee on Commercial and Administrative Law, "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security", February 10, 2004.

[151] DHS, *PIA Update*, op. cit.,1 July 2005, p. 2.

incrementally as different technology solutions must be in place to implement different parts. Many of the privacy issues discussed in the PIA report are specific to individual stages of implementation as different technologies and systems collect, process and store different elements of personal information.

The personal information used

As part of the US-VISIT programme, the DHS has been collecting since 2004 biometric information from travellers to the US, including two digital index finger scans and a digital photograph, and personal information such as complete name, date of birth, gender, country of citizenship, passport number and country of issuance, country of residence, travel document type (e.g., visa), number, date and country of issuance, complete US destination address, arrival and departure information. In the first phase, information was collected from non-US citizens entering the USA. In the second part of phase one, this information was matched to databases including the Automatic Biometric Identification System (IDENT) and other databases that hold information about criminal activity, immigration-related offences and terrorist watch lists. In the second phase, information was also collected when those visiting the US exited the country, and this resulted in a modification of IDENT to forward departure information to a system called the Arrival and Departure Information System (ADIS). In the third part of phase two, this biographic and biometric information collection will be expanded to provide a capability to "automatically, passively, and remotely record the entry and exit of covered individuals using Radio Frequency Identification (RFID) tags" in US-issued immigration documents.[152] A unique identifier in the tag will be used as a record number for the individual's biographic information stored in the Treasury Enforcement Communications System (TECS) database and linked with ADIS. When an individual passes through an entry or exit lane of a point of entry, the ID number embedded in the immigration document will be read and it will be used to retrieve the biographical information which will then be fed to customs and border officials once the individual approaches the official.

How is the information being shared, used and retained?

The PIA report states that US-VISIT shares information with other DHS systems for purposes such as status updates and benefit adjudication, national security and law enforcement. The system architecture section includes a detailed data flow chart demonstrating how information flows between different components of the system. The report states that employees of other DHS divisions, such as Customs and Border Protection, Immigration and Customs Enforcement, and the Department of State can access some of the information collected and maintained by US-VISIT.

General privacy issues and risks identified

The US-VISIT PIA identifies various privacy and security risks. One of the primary privacy issues relates to information security, where the intentional or unintentional unauthorised access to information represents an area of significant discussion in the PIA report. In fact, Appendix D (Security Safeguards for Privacy Protection Detailed) and Appendix E (Privacy Threats and Mitigations) only mention risks related to information security and unauthorised access. However, the document does mention other general privacy issues, including privacy issues related to information sharing, consent, notice or awareness, access or participation and redress. The PIA states that these privacy risks are mitigated by an agency privacy policy that

[152] Ibid., p. 7.

is "supported and enforced by a comprehensive privacy programme".[153] The document also gives the Web address for the privacy policy.

General resolutions identified

General resolutions to these non-specific risks include the use of data-sharing agreements, staff training, periodic assessment and PET-type system modifications. Data-sharing agreements should ensure that other law enforcement partners, contractors or consultants address privacy and security concerns and implement operational requirements for sharing, including signing a non-disclosure agreement in some cases. Staff training will ensure that users are trained regarding the security of their systems and privacy issues. Periodic assessments will examine the effects of physical, technical and administrative controls on accountability and data integrity.[154] Privacy-enhancing systems such as strong access controls, limited retention of data, limited collection of data and encryption can assist in providing robust privacy protection. Finally, the PIA mentions that US-VISIT has a redress policy, to which the PIA report provides a link and states that the privacy officer aims to process redress requests within 20 business days.

Specific risks and resolutions

In addition to the general threats and solutions identified in the PIA report, the document lists specific privacy risks and resolutions in relation to particular implementations of the US-VISIT programme.

In relation to the exit kiosk in which travellers register their departure from the USA, the PIA report recognises a low potential security risk that an individual may be persuaded by someone masquerading as an authorised official to submit their personal information and fingerprints to a counterfeit device. This risk is mitigated by staff training, awareness measures for travellers describing precise situations in which they will be asked to provide personal information and security measures to prevent unauthorised individuals from accessing airport spaces. Another privacy risk associated with exit kiosks is the potential for the personal information included on receipts issued by the kiosks to be intercepted by an unauthorised individual. Solutions to this risk include minimising the amount of human readable information by translating information into a bar code, minimising the biometric information on the receipt and encrypting biographic and biometric information.[155] Finally, fingerprint and biographic information is temporarily stored on the exit devices before being transmitted to a server, and upon transmission to the server, the information on the kiosk is permanently deleted. However, because the exit kiosk retains the information if a malfunction occurs, all personal information stored on an exit kiosk is encrypted to ensure information security.

The PIA also identifies specific privacy and security risks and resolutions in respect of the implementation of RFID-embedded immigration documents. The PIA states that while RFID tag numbers are not encrypted, the RFID tag does not contain personal information and can only be used to obtain personal information in combination with the associated database. This Automated Identification Management System (AIDMS) database can "only be accessed by authorized personnel signed into authorized workstations that communicate with the AIDMS

[153] Ibid., p. 12.
[154] Ibid., p. 11.
[155] Ibid. p. 13.

via a secure network".[156] Furthermore, the AIDMS database only records entry and exit data for a particular RFID tag, while the TECS database holds the biographic information. This separation of data increases security and privacy. The PIA also identifies a low risk that the RFID system could be used for locational surveillance of an individual as he or she moves about the US, but the use of a limited radio frequency mitigates this risk and further design processes are researching methods to reduce the risk of data eavesdropping and skimming.

In relation to retention periods, the PIA report also notes that different components of the US-VISIT programme have different retention periods published in their associated System of Records Notices (SORNs). This could result in a heightened degree of insecurity or an access or redress risk as personal information deleted in one system could remain in an associated system. The PIA report states that "a comprehensive assessment of retention requirements has been initiated" as a result.[157]

Finally, the PIA report notes that DHS considered the use of GPS technology and active RFID systems[158] rather than passive RFID technology, but both were abandoned due to privacy risks.[159]

The US-VISIT PIA offers the following points in conclusion:

- While most of the initial high-level design choices for US-VISIT were statutorily predetermined, more recent design choices have been made so that privacy risks are either avoided or mitigated while meeting operational requirements.
- US-VISIT creates a pool of individuals whose personal information is at risk (covered individuals), which is effectively growing as a result of the expanded functionality, data sharing and implementation of US-VISIT, but
- US-VISIT mitigates the specific privacy risks associated with its new functionality and increased data sharing through numerous mitigation efforts, including access controls, education and training, encryption, minimising collection and use of personal information.
- US-VISIT through its Privacy Officer and in collaboration with the DHS Chief Privacy Officer will continue to track and assess privacy issues throughout the life of the US-VISIT Program and will address those issues by adjusting existing and implementing new privacy risk mitigations as necessary.[160]

9.11.1 Effectiveness

Although shortcomings of DHS privacy impact assessments were discussed in the previous section, the US-VISIT PIA represents a relatively effective assessment of privacy risks and mitigations. Using our criteria set out in section 9.1 above yields the following results:

Did the PIA report	
clarify whether the PIA was initiated early enough so that there was still time to influence the design of the project (or even whether the project should proceed at all)?	Yes
identify who conducted the PIA?	Yes
include a description of the project to be assessed, its purpose and any relevant contextual information?	Yes

[156] Ibid., p. 13.
[157] Ibid., p. 14.
[158] Active RFID systems have their own power source and constantly transmit signals, while passive RFID systems require an authorised reader to activate the tag in order to read data from it.
[159] Ibid., p. 17.
[160] Ibid., pp. 17-18.

Did the PIA report	
map the information flows (i.e., how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)?	Yes
check the project's compliance against relevant legislation?	Yes
identify the risks to or impacts on privacy?	Yes
identify solutions or options for avoiding or mitigating the risks?	Yes
make recommendations?	No
get published on the organisation's website? Is it easily found there? If the PIA report was not published (even in a redacted form), was there an explanation as to why it has not been published?	Yes
identify what consultation was undertaken with which stakeholders?	Yes, but only generally

In addition to covering all but one of the criteria mentioned in section 10.1, the efficacy of this document has also been recognised by privacy experts. James Dempsey of the Center for Democracy and Technology calls the US-VISIT PIA "an important document and has served to bring greater transparency to that program"[161] and applauds the document for its "forthrightness and clear analysis of those issues as well as the detailed description of how the program will function"[162].

One of the strong points of the US-VISIT PIA report is that it is a living document which has been updated as the US-VISIT system has expanded and changed. Thus, many of the aspects of the programme could be commented upon before the system was fully implemented, particularly while it was in the testing phase. The document is also fairly clear about what general and specific privacy issues are raised by the programme and discusses many of the ways in which these are mitigated. Furthermore, although it does focus primarily on information security, locational surveillance was also identified as a privacy risk. Finally, some consultation mechanisms were undertaken by the DHS and changes have resulted from this. For example, concerns about the lack of a redress mechanism in earlier versions of the PIA resulted in a clearer statement about redress in this updated version.

9.11.2 Shortcomings

Yet, despite these strengths, the US-VISIT PIA has shortcomings. First, it does not invite or make recommendations as to how the programme could be improved, it simply states which resolutions were implemented by the DHS. Second, although the PIA mentions locational surveillance, the risk analysis is focused on intentional or unintentional data security breaches by authorised or unauthorised persons. There is only a very brief discussion of privacy threats for individuals whose data is in the system as a result of misuse or poorly designed features. Thus, the threat to privacy appears to be perceived as external rather than internal. The US-VISIT PIA also does not invite public or expert comments on the PIA or the programme itself, thus the PIA appears to exist as a dissemination document only. Finally, although the PIA recognises that the data retention periods are varied across the programme, the Center for Democracy strongly criticises the DHS for not stating what the retention periods of the

[161] Dempsey, op. cit., 2004.
[162] Center for Technology and Democracy, Comments of the Center for Technology and Democracy on US-VISIT Program, Increment 1, Privacy Impact Assessment (December 18, 2003), 4 Feb 2004, p. 1.

different information systems are, leaving individuals to trawl through the individual SORNs, and for having an unclear policy for ensuring the quality of the data they collect.[163]

[163] Center for Democracy and Technology, op. cit., 2004.

10 CONCLUSIONS

In this chapter, we present our conclusions from the review and analysis of PIA methodologies, policies and practices in Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and US as well the 10 case studies of PIA reports in Australia, Canada, New Zealand, the UK and US. We also make some comparisons between the methodologies and case studies.

Before doing so, however, we think it is useful to emphasise the benefits of PIA to organisations, from the both the public and private sectors. The following section presents a synthesis of some of the principal benefits mentioned in some of the PIA guidance documents. We think it is useful to emphasise these benefits because some organisations may view PIA as an undue burden, when (so we believe) they should instead view PIA as a way to save themselves money and embarrassment and avoid damage to their reputation.

10.1 WHY SHOULD AN ORGANISATION UNDERTAKE A PIA?

While a privacy impact assessment is a methodology for identifying risks to privacy posed by any new project, product, service, technology, system, programme, policy or other initiative and devising solutions to avoid or mitigate those risks, it also offers several important benefits to organisations, their employees, contractors, customers, citizens and regulators. Among them are the following:

A PIA has often been described as an early warning system. It provides a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments. The costs of fixing a project (using the term in its widest sense) at the planning stage will be a fraction of those incurred later on. If the privacy impacts are unacceptable, the project may even have to be cancelled altogether. Thus, a PIA helps reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early. It helps an organisation to avoid costly or embarrassing privacy mistakes.

Although a PIA should be more than simply a compliance check, it does nevertheless enable an organisation to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation. In the event of an unavoidable privacy risk or breach occurring, the PIA report can provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.[1]

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions about the project. A PIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers. A PIA functions as a credible source of information. It enables an organisation to learn about the privacy pitfalls of a project, rather than having its critics or competitors point them out. A PIA assists in anticipating and responding to the public's privacy concerns.

[1] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010, p. 14.

A PIA can help an organisation to gain the public's trust and confidence that privacy has been built into the design of a project, technology or service. Trust is built on transparency, and a PIA is a disciplined process that promotes open communications, common understanding and transparency. An organisation that undertakes a PIA appropriately demonstrates that the privacy of individuals is a priority for their organisation. It affirms that an organisation has addressed privacy issues and has taken reasonable steps to provide an adequate level of privacy protection.

An organisation that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them to do so too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that might damage the organisation. It is a way to affirm the organisation's values.

A proper PIA also demonstrates to an organisation's customers and/or citizens that it respects their privacy and is responsive to their concerns. Customers or citizens are more likely to trust an organisation that performs a PIA than one that does not. They are more likely to take their business to an organisation they can trust than one they don't.

We assume regulators are likely to be more sympathetic towards organisations that undertake PIAs than those that do not.

10.2 A COMPARISON OF PIA POLICIES AND PRACTICES IN THE SURVEYED COUNTRIES

The table on the following two pages identifies similarities and differences between the principal PIA guidance documents analysed in this deliverable. (Those of Hong Kong and the UK Department of Justice have not been included as they are significantly less developed than those covered in the table below.)

Table 10.1 – Similarities and differences between PIA policies and practices

Features The PIA guide…	Australia	Victoria	Canada	Ontario	Alberta	Ireland	NZ	UK ICO	US OMB	US DHS
reviewed here, was published in	May 2010	Apr 2009	Aug 2002	Dec 2010	Jan 2009	Dec 2010	Oct 2002-2007	June 2009	Sept 2003	June 2010
says PIA is a process	✓	✓	✓	✓		✓	✓	✓	✓	✓
contains a set of questions to uncover privacy risks (usually in relation to privacy principles)	✓	✓	✓	✓		✓	✓	✓		✓
targets companies as well as government	✓	✓			✓	✓	✓	✓		
addresses all types of privacy (informational, bodily, territorial, locational, communications)	✓	✓		✓						
regards PIA as a form of risk management	✓		✓	✓		✓		✓	✓	✓
identifies privacy risks	✓	✓	✓	✓		✓	✓	✓		
identifies possible strategies for mitigating those risks		✓					✓			
identifies benefits of undertaking a PIA	✓	✓	✓			✓	✓	✓		
supports consultation with external stakeholders	✓	✓				✓		✓		
encourages publication of the PIA report	✓	✓	summary		summary		✓	✓	✓	✓
provides a privacy threshold assessment to determine whether a PIA is necessary	✓	✓	✓			✓		✓	✓	✓
provides a suggested structure for the PIA report	✓	✓	✓		✓		✓	✓	✓	✓
defines "project" as including legislation and/or policy		✓								
says PIAs should be reviewed, updated, ongoing throughout the life a project	✓	✓			s✓	✓	✓	✓	✓	✓
explicitly says a PIA is more than a compliance check	✓	✓	✓	✓				✓		
The PIA policy provides for third-party, independent review or audit of the completed PIA document.			✓		✓		✓		✓	✓
PIA is mandated by law, government policy or must accompany budget submissions.			✓	✓	✓	✓		✓	✓	✓
PIA reports have to be signed off by senior management (to foster accountability).		✓	✓	✓	✓	✓			✓	✓

10.3 BEST ELEMENTS

In each of the country chapters, we identified the elements that we most liked and would recommend for a European PIA policy and methodology. For the reader's ease of reference, we summarise and synthesise here those elements:

PIA guidance documents should be aimed at not only government agencies but also companies or any organisation initiating or intending to change a project, product, service, programme, policy or other initiative that could have impacts on privacy.

PIAs should be undertaken with regard to any project, product, service, programme or other initiative, including legislation and policy, which are explicitly referenced in the Victoria Guide and the UK Information Commissioner's Office (ICO) Handbook.

Information privacy is only one type of privacy. A PIA should also address other types of privacy, e.g., of the person, of personal behaviour, of personal communications and of location.

The Victoria Guide points out that a project need not be large to be subject to a PIA, nor is the size or budget of a project a useful indicator of its likely impact on privacy. The project does not even need to involve recorded "personal information"; for example, a program that may include the need for bodily searches can still impact on privacy even if no personal information is recorded.

The PIA should identify information flows, i.e., who collects information, what information do they collect, why do they collect it, how is the information processed and by whom and where, how is the information stored and secured, who has access to it, with whom is the information shared, under what conditions and safeguards, etc.,

A PIA guidance document should include an indicative list of privacy risks an organisation might encounter in initiating a new project, but should caution project managers and assessors that such a list is not exhaustive. The questions most PIA guidance documents include can help stimulate consideration of possible privacy impacts.

A PIA is more than a check that a project complies with existing legislation or privacy principles. A PIA should include a compliance check, but it should go beyond a simple compliance check and engage stakeholders in identifying risks and privacy impacts that may not be caught by a compliance check. The purpose of a PIA is to identify and resolve privacy impacts, not simply to ensure that a project complies with legislation.

A PIA is also different from an audit. A PIA is used to identify risks and solutions to those risks, whereas an audit is used to check that the PIA was properly carried out and its recommendations implemented (or, if some are not implemented, then an adequate explanation as to why they were not).

Several of the PIA guidance methodologies (e.g., Australia, UK) say that "Consultation with stakeholders is basic to the PIA process." The UK provides more guidance than most with regard to consultation with stakeholders. The UK Ministry of Justice PIA guidance describes consultation of stakeholders as a "core element".

Engaging stakeholders, including the public, will help the assessor to discover risks and impacts that he or she might not otherwise have considered. A consultation is a way to gather fresh input on the perceptions of the severity of each risk and on possible measures to mitigate these risks. Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report. The ICO says the PIA process inform or be embedded as part of the consultative process of public sector projects, many of which are obliged to consult stakeholders, including the public.

A PIA should be started early, so that it can evolve with and help shape the project, so that privacy is "built in" rather than "bolted on". A PIA should be initiated when it is still possible to influence the design of a project. The findings and recommendations of the PIA should influence the final detail and design of the project.

Although many of the PIA guidance documents, such as the Ontario Guide, the New Zealand Handbook and the ICO Handbook, say that "no one size fits all" in PIA, that organisations should use the guidance document to guide their PIA process in a manner "appropriate to their circumstances", most guidance documents offer a structured approach to the PIA process and preparation of a PIA report. In the case of Alberta, the format is mandatory.

The Irish Health Information and Quality Authority has developed a sample PIA report based on its Guidance to help assessors. The Victoria Privacy Commissioner includes a template that provides the structure of a PIA report, which the user can adapt to his or her circumstances. The template has been produced as a Word document for ease of use by the assessor. PIA guidance should include a specific template to guide and assist staff in producing comprehensive PIA reports.

A project manager or whoever leads a PIA typically needs to bring together different skill sets in order to carry out the PIA. A guidance document will help the project manager when it identifies the variety of skills required for undertaking a privacy impact assessment and completing a privacy impact report, when it highlights the importance of bringing together people with the right competencies to be members of the PIA team and to conduct a PIA.

Questionnaires are helpful in stimulating consideration of privacy impacts, but they become mere checklists if respondents only have to answer yes or no. The best questionnaires require some explanation or details of how the PIA addresses the issues raised by each question.

The ICO Handbook emphasises PIA as a process, not simply an exercise aimed at producing a report. The objective of a PIA is not simply to produce a PIA report. The report documents the PIA process. A PIA should continue after the report is published. PIAs should be embedded as part of the project management framework. The PIA should be reviewed and updated throughout the duration of a project. The UK's Ministry of Justice conceptualises the PIA process as a "living" document.

A PIA report should normally be publicly available and posted on an organisation's website so as to increase transparency and public confidence. If there are security, commercial-in-confidence or other competitive reasons for not making a PIA public in full or in part, the organisation should publish a redacted version or, as a minimum, a summary. The public has a right to know if their privacy will be impacted by a new project or changes to an existing project. A properly edited PIA report will usually suffice to balance the security and transparency interests.

Data protection authorities (privacy commissioners) should make it easy for project managers, assessors and others to find a link for downloading the PIA guidance, preferably on their home page. Some PIA documents (e.g., that of Ontario) are quite hard to find.

A PIA guidance should include a list of references to other PIA guidance documents and actual PIA reports. It should draw on the experience of others to make the Guide more practical and effective. The New Zealand handbook has a useful bibliography of national and international PIA resources.

Governments especially should create a central registry of PIAs, so that particular PIA reports can be easily found. Publication of PIA reports will enable organisations to learn from others.

The guidance document should not only set out various risks, but also possible strategies for mitigating those risks, as the ICO and Victoria PIA guidances do. But, again, such lists of risks should only be regarded as indicative, not exhaustive.

A PIA guidance should include a threshold assessment, the aim of which is to help project managers determine whether a PIA is needed.

PIA should have up-front commitment from an organisation's senior management. Senior management should be held accountable for the proper conduct of a PIA and should sign off the PIA report, as the Treasury Board Secretariat (TBS) of Canada requires. Funding submissions should be accompanied by a PIA report. TBS policy also requires that government departments and agencies copy the PIA report to the Privacy Commissioner, which we also find to be a good practice.

A PIA guidance document should be updated from time to time, as has happened in several countries.

PIA should be part of an organisation's overall risk management practice.

As many organisations, especially those from the private sector, may resist undertaking a PIA, a guidance document should highlight the benefits of undertaking PIAs and how they will help an organisation.

In New Zealand, PIA is regarded as an "early warning system". Other PIA guidance documents have picked up on the same wording.

PIAs should be applied to cross-jurisdictional projects as well as individual projects. PIAs should invite comments from privacy commissioners of all jurisdictions where projects are likely to have significant privacy implications and ensure that such projects meet or exceed the data protection and privacy requirements in all the relevant countries.

Privacy commissioners do not generally approve PIAs; however, they may review them and provide guidance on improving them.

PIA reports and practices should be audited, just as a company's accounts are audited. An audit will help improve PIA practice, as the Office of the Privacy Commissioner of Canada found following its major audit of PIAs in 2007. To increase their effectiveness, PIAs should be subject to external oversight.

In addition to PIA guidance documents, the government of Canada developed a PIA Audit Guide, "intended as a reference tool for Internal Auditors in the Government of Canada and may also be of assistance to the privacy community, including PIA Coordinators". Others could do so too.

Privacy commissioners or other leaders should identify and publish particular PIA reports as examples of good practice.

A PIA in its own right may not highlight all privacy risks or issues associated with an initiative. A successful PIA is only a tool; its utility depends on how it is used and who uses it. It depends on service providers having the correct processes in place to carry out the PIA. These include identification of the correct stakeholders for the assessment, selection of those with the necessary knowledge and skills to carry out the PIA and involvement of senior managers in order to implement the PIA recommendations.

The PIA should be reviewed and approved at a senior level with each PIA report being quality assured by senior management.

Service providers should routinely undertake a threshold assessment for every new project as well as proposals to amend existing information systems, sources or processes to determine whether its potential privacy impact necessitates a PIA.

The focus of a PIA report should be on the needs and rights of individuals whose personal information is collected, used or disclosed. The proponent of a proposal is responsible for privacy. The proponent must "own" problems and devise appropriate responses in the design and planning phases.

The PIA should specify who undertook the PIA and how they can be contacted for more information and where to find further information and other sources of help and advice.
US experience suggests the value of ensuring the chief privacy officer has a senior position, has a high degree of independence within the organisation and participates in high-level deliberations. A chief privacy officer, privacy office and/or PIA process should be statutorily mandated by an external agency. An adequate number of specially trained privacy-focused staff members should be embedded throughout the organisation.

10.4 CONCLUSIONS FROM THE CASE STUDIES

This chapter analysed 10 PIA reports – two each from Australia, Canada, New Zealand, UK and the US. The following table compares these reports based on the evaluation criteria in 9.1.

Table 10.2 – Comparison of PIA reports

Evaluation Criteria	EVI [AU]	Ultranet [AU]	Infoway EHR [CA]	EDL [CA]	Biometrics [NZ]	Google Streetview [NZ]	iACT [UK]	CSO Disclosure Scheme [UK]	Fusion Centres [US]	US-VISIT [US]
Clarification of early initiation	✓	✓	✓	✓	✓	X	✓	X	✓	✓
Identification of who conducted PIA	✓	✓	✓	✓	✓	X	✓	✓	✓	✓
Project description, purpose and relevant contextual information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Information flow mapping	✓	✓	✓	✓	✓	✓	✓	✓	X	✓
Legislative compliance checks	✓	✓	✓	✓	✓	X	✓	✓	✓	✓
Identification of privacy risks and impacts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identification of solutions/options for risk avoidance, mitigation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recommendations	✓	✓	✓	✓	✓	✓	✓	X	✓	X
Publication	✓	Executive Summary	✓	X	✓	✓	✓	✓	✓	✓
Identification of stakeholder consultation	✓	Not apparent from Exec. Summary	X	X	✓	X	✓	X	✓	✓

The analysis of the PIA reports against the evaluation criteria reveals a very interesting picture. All the PIA reports commonly contain, in some form and varying degree, the following: a project description, purpose, relevant contextual information, identification of privacy risks and impacts and identification of solutions or options for risk avoidance and mitigation.

In relation to the other report evaluation criteria, there were significant differences in practice. PIA reports vary as much between jurisdictions as within. For example, the full report of the Australian Electronically Verifying Identity PIA is publicly available on the Web, yet the Australian PIA report on the Ultranet ICT Project for Schools is not (only an executive summary is available). The Canadian PIA report on Infoway Electronic Health Records (EHR) covers stakeholders and stakeholder consultation in only a limited way while the Canadian PIA report on the Enhanced Driver's Licence gives a good description of stakeholders and stakeholder consultation. This shows that practice in relation to PIA reports varies vastly.

Best features

The best features that emerge from the overall analysis of the PIA reports are: envisaging the PIA as an iterative process, implementing a PIA report as a living document; publication of the full PIA report; readability and accessibility of the report; inclusion of details of who conducted the PIA and who can be contacted for further information; and adequate identification of privacy threats, and incorporation of responses to recommendations. Thus, there is something positive to be said about PIA reports overall.

Areas of improvement

The PIA reports analysed present some areas for improvement.

The first relates to the provision of adequate contextual information in the PIA report. The New Zealand PIA report on the Collection and Handling of Biometrics at Department of Labour and the UK CSO Disclosure Scheme PIA report lack clarity about the timing and duration of the PIA. Other PIA reports such as the Canadian Enhanced Driver's Licence PIA fail to specify for whom the PIA report is intended, its proposed use and how its recommendations will be monitored. The New Zealand Google Street View PIA report fails to identity who conducted and authored the PIA, does not provide information on the duration of the PIA, nor outline the assumptions underlying the assessment or the terms of reference.

Even though stakeholder consultation is a crucial element of the PIA process,[1] PIA reports often fail to acknowledge this, or give it limited berth – as evident in the case of the Australian PIA report on the Ultranet ICT project for schools[2] and the Canadian Infoway electronic health records (EHR) PIA. At other times, details on stakeholder consultations are lacking, as in the case of the New Zealand Google Street View PIA. Sometimes, reports fail

[1] Earlier, we conceptualised a PIA as "a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts". Section 1.2 of the Deliverable. Definition adopted in Wright, David, and Paul De Hert, "Introduction to privacy impact assessment" in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

[2] Recall that the Australian Privacy Commissioner (OPC) PIA Guide regards consultation with external stakeholders, including the public, as an element in good PIA practice.

to adequately identify stakeholders – e.g., the Canadian Health Infoway Electronic Health Records (EHR) and the UK CSO Disclosure Scheme PIA reports.[3]

The next overall concern relates to the publication and dissemination of PIA reports. As discussed earlier, PIA reports are hard to find. It is easier to find PIA reports for the public sector; private sector reports are very hard to come by. This makes it difficult to get a true picture of the nature of PIAs and makes transparency and accountability[4] hard to achieve. In the case of our examples, only the Executive Summary was available for the Australian Ultranet PIA.[5] The Canadian Enhanced Driver's Licence PIA report was not published on the CBSA's website and it is not clear where one can find the PIA report on the Collection and Handling of Biometrics on the New Zealand Department of Labour's website. The publication and dissemination of PIA reports is in the public interest – not only to generate transparency and accountability, but also to enable other organisations to draw upon and learn from these reports in order to improve overall PIA culture. PIA reports must not simply function as organisational public image enhancement tools.

Mapping information flows is crucial to determining the privacy impact of a project. The US DHS Fusion Centers PIA demonstrates shortcomings in this respect. It fails to provide details on personal information collection, sharing and retention. The US-VISIT PIA report too has been criticised for failing to provide specific details about retention periods of the different information systems.[6]

10.5 LEGAL OBSERVATIONS

Strong evidence for PIA has been found in thirteen jurisdictions[7] worldwide. Seven of them are sovereign states (Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and the US). Five of them are constituent countries of independent states (Australian Victoria; Canadian: Alberta, British Colombia and Ontario; and Ohio in the US). One of them is a regional supranational jurisdiction (the EU), covering also two independent states (Ireland and the UK).

There are substantial differences in PIA methodology (legal aspects, practice, policy, etc.) in the above-mentioned jurisdictions. They have different approaches to privacy and protection of personal data. There is a different understanding what PIA exactly means. This is reflected in scope of PIA as it mostly covers informational privacy and not all privacy aspects (e.g. bodily or territorial privacy). The concept of PIA is developing, e.g. new legislative initiatives are undertaken and new editions of guidance material are published.

The starting point here is a PIA (legal) basis as the likelihood of PIAs being conducted is a function of the policy compulsion to undertake them.[8] These bases fall into at least four

[3] Note that the UK ICO *PIA Handbook* also emphasises consultation with external stakeholders
[4] Values incorporated in most PIA Guidance. See the Australian OPC PIA Guide (p. x); the OVPC PIA Guide (p. 18); the Irish PIA Guidance; the UK MOJ Guidance (p. 14) and the UK ICO Guidance.
[5] Recall the discussion in Section 3.4 about the problems of obtaining full PIAs: delays, fees and severing or redacting of information.
[6] See section 9.11.2 of the Deliverable.
[7] A jurisdiction might be defined as territorial unit within which a court or government may properly exercise its power.
[8] Bayley, Robin, and Colin J. Bennett, "Privacy impact assessments in Canada", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012 [forthcoming].

categories: hard law,[9] soft law, public guidance material and – additionally – normative proposals. However, sometimes it is difficult to ultimately assess the "strength" of a normative instrument as it highly depends on a respective constitutional system.

First, only seven jurisdictions have an explicit and strong legal basis for PIA (hard law): the US and the US state of Ohio; Canada (federal) and three Canadian provinces: Alberta, British Colombia and Ontario; and New Zealand. No legal instrument at the international level for PIA has been found. However, a legal basis for PIA could be also found in by-laws (e.g. codes of conduct), e.g. in Australia.

These legal bases vary considerably. Taking into consideration the normative hierarchy, PIA is usually mandated by a legal statute (i.e. an act of a parliament), but in Canada (federal) – by a legal instrument on the level of ministers (i.e. delegated power). Some legal provisions specify a PIA in a great detail, e.g. the obliged entity/authority, procedure, content of a PIA report, supervision or publication. Some just mention its compulsory nature only. (Compare e.g. the US E-Government Act and the Homeland Security Act.) Sometimes non-compliance with a PIA requirement is specifically sanctioned, e.g. Canada (federal). When it comes to terminology, quite interestingly, in one case, PIA was not referred to explicitly, by its name, i.e. the laws of Ontario provide for the "*assessment … with respect to … how the services may affect the privacy of the individuals*."

In case PIA is mandated by law, these laws usually create a legal obligation that binds public sector only. An exception is the health sector in some jurisdictions, where all actors processing personal information are obliged to conduct PIA, if applicable. Furthermore, PIA legal bases are not usually of a general nature, but sector-specific only, e.g. in the US it is mandated for e-government and for homeland security purposes, in Ohio – for confidential personal information (e.g. medical data), in Alberta and Ontario – for electronic health records, and in New Zealand – for biometric data for immigration purposes. For most of them, the common denominator is the impact of emerging technologies. Only Canadian (federal) and British Colombia's PIA methodologies can be seen as of a general nature within public sector.

It is worth mentioning that majority of jurisdictions analysed have mandated by law some tools that share certain characteristics with PIA, predominantly a form of prior checking (of proposed processing operations), i.e. the EU, Ireland, and the UK, or a form of prior consultation (of proposed legislation, data matching programme, etc.). What all these tools have in common with PIA is the *ex ante* examination. Clarke has identified these notions as pre-dating PIAs and on which the formulation of PIA processes was based.[10]

Second, PIA is mandated by soft law in two jurisdictions. In the EU, the RFID PIA Recommendation has a normative value, but it does not constitute any legal obligation and is not enforceable. The UK report on data handling procedures in government requires PIA be conducted, but it does not have legal force and thus it constitutes only an internal policy. In

[9] However, for the purposes of this deliverable, the category of "hard law" consists of all four major types of legal norms: *lex plus quam perfecta* (non-compliance results in sanction and invalidity), *lex perfecta* (invalidity), *lex minus quam perfecta* (sanction), and *lex imperfecta* (no sanction). Note also that privacy and data protection legislation contains their own general provisions sanctioning non-compliance.

[10] Clarke, Roger, "Privacy impact assessment: Its origins and development," *Computer Law & Security Review*, Vol. 25, No. 2, 2009, p. 123.

addition, the Commission's impact assessment – containing only a tiny privacy and data protection component – could be conceptualised as soft constitutional law.[11]

Third, in seven jurisdictions, a PIA guidance material issued by a privacy and data protection authority (information commissioner) serves as a *sole* PIA basis, i.e. in Australia (federal), Australian state of Victoria, Hong Kong and Ireland. Therefore, it is fair to conclude that it is not mandated by law, it is only recommended, and thus it shares some characteristics with soft law. In the EU, New Zealand and the UK, a legal basis and a PIA guidance material co-exist (see *infra*). In any case, they help in undertaking PIA (e.g. by providing explanation and/or templates). Additionally, PIA guidance material is sometimes issued by private sector, e.g. in Canada.[12] On the other hand, the EU RFID PIA guidance is a fruit of cooperation of both public and private stakeholders. (The Commission asked "*the industry in collaboration with relevant civil society stakeholders.*") This remark is vital for the discussion of the source of PIA guides.

In Canada (federal), Ontario, New Zealand, the UK and the US, both public guidance material and a legal basis for PIA co-exist. Sometimes they are independent from each other, sometimes they overlap, and sometimes they specify the PIA requirement in a greater detail. In New Zealand, there is a general 2008 PIA handbook, but 2009 legislation focuses only on a specific sector, i.e. biometrics. The UK introduced a policy within government to undertake PIA, but the PIA guidelines are a separate "story". In Ontario, both types focus on health information, yet the guidelines emphasise those actors for whom PIA is compulsory. The US guidance material is issued separately by a number of federal agencies pursuant to the both Acts.

Soft law, despite its possible compliance drawbacks (neither binding nor enforceable), has its own benefits, e.g. its flexibility. It can explain in which manner a public body will interpret a legal statute, if a soft law instrument is issued pursuant to such legislation. A PIA report conducted under a soft law requirement could serve as evidence, *cf.* a statement in a PIA guide in Ontario: "the IPC may use any PIA as a starting point for any investigation into a breach of privacy."

Fourth, some jurisdictions have introduced a PIA requirement into their regulatory frameworks for protection of privacy and personal data, i.e., Australia (federal), Canada (federal), Ireland, the UK and the EU. Yet these vary considerably. In the case of Canada, the proposal aims at strengthening the obligation to undertake a PIA, predominantly by placing a PIA requirement into a legal statute and not only in a ministerial instrument. In addition to the jurisdictions examined, Finland and the Netherlands consider introduction of PIA policy.[13] Also, the Council of Europe's Additional Protocol to Convention No. 108 can be seen as "permitting" and "encouraging" PIA, cf. "intervention and investigation powers" of DPAs (in the light of the explanation given to this provision). In addition, the Council's documents suggest PIA introduction.

To sum up:

PIA feature	AU	CA	EU	HK	IE	NZ	UK	US

[11] Meuwese, A., *Impact Assessment in EU Lawmaking*, Ph.D. Thesis, University of Leiden, 2008, pp. 102-104. https://openaccess.leidenuniv.nl/bitstream/handle/1887/12589/Thesis.pdf?sequence=3

[12] In addition, Clarke has published his own set of PIA guidelines: http://www.xamax.com.au/DV/PIA.html

[13] Cf. http://www.piawatch.eu/pia-country

hard law		X+3				X		X+1
soft law			X				X	
guidance only	X+1	X		X	X	X	X	
guidance		+1	X					X
proposals	X	X	X		X		X	

ANNEX 1 – LEGAL BASES FOR PIA AT THE EUROPEAN LEVEL

EUROPEAN UNION

1. General framework for privacy and data protection

Protection of privacy and personal data in the European Union is based on its Treaties, the Charter of the Fundamental Rights (CFR) and secondary legislation, namely the Directives (see *infra*). After the entry into force of the Lisbon Treaty (2009), the CFR became a legally binding instrument and the Treaties now include explicit reference to protection of personal data. Art. 16 (*ex* Art. 286) of Treaty on the Functioning of the European Union (TFEU) and Art. 39 of Treaty on the European Union (TEU) both recognise the right to data protection. Art. 7 of CFR provides for the right to respect for private and family life and Art. 8 provides for the protection of personal data.

The Court of Justice of the European Union in Luxembourg (colloquially the European Court of Justice, ECJ) ensures uniform application of the EU law. The court has delivered a number of landmark decisions regarding privacy and data protection, e.g. *Lindqvist* (C-101/01), *Promusicae* (C-275/06) or *Bavarian Lager* (T-194/04).

The EU secondary legislation consist of three "basic" instruments: **Data Protection Directive** (95/46/EC),[1] **ePrivacy Directive** (2002/58/EC),[2] as amended by Directives: 2006/24/EC and 2009/136/EC,[3] and **Data Retention Directive** (2006/24/EC).[4]

The "specific" instruments consist of the Council Framework Decision 2008/977/JHA[5] (dealing with data protection with regard to criminal matters, i.e. former 3rd pillar) and the Regulation 45/2001[6] (lying down data protection rules for the EU institutions and bodies). The European Commission recently launched the process of the revision of these instruments.[7]

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[3] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[5] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[6] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[7] *Cf.* the Communication "A comprehensive approach on personal data protection in the European Union", COM (2010) 609 final. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf. Note also that the Council of Europe considers the revision of the Convention No. 108 upon its 30th anniversary of signature (cf. http://www.coe.int/t/dghl/standardsetting/dataprotection/Modernisation_en.asp). The OECD has said much the same thing with regard to its 1980 Privacy Guidelines.

2. Laws on PIA forerunners

Art. 20 of the Data Protection Directive establishes **prior checking**:

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

A 2007 study conducted for the Information Commissioner's Office (ICO) in the UK overviews how the EU Member States implemented Art. 20 in their national legislation.[8] According to the Report, a majority of Member States implemented some form of prior checking. The report further comments (p. 4) that:

> the primary legislation defines the categories of processing operations that will be subject to prior checking, but sometimes the law provides that secondary legislation will define which processing operations should be subject to prior checking. The degree to which prior checking is used across the Member States varies widely.

Next, Art. 28 empowers a national supervisory authority with **prior consultation** functions:

> 2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.
> 3. Each authority shall in particular be endowed with:
> …
> – effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions

Similar powers are vested to the Art. 29 Working Party with regard to the EU regulatory framework for data protection (Art. 30):

> 1. The Working Party shall:
> (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
> (b) give the Commission an opinion on the level of protection in the Community and in third countries;
> (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard

[8] Information Commissioner's Office, *Privacy Impact Assessments: International Study of their Application and Effects*, Appendix H: *Broad Jurisdictional Report for the European Union*, 2007, pp. 4-9, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
(d) give an opinion on codes of conduct drawn up at Community level.

Regulation 45/2001, regulating processing of personal data by EU institutions and bodies, empowers the European Data Protection Supervisor (EDPS) with **prior checking** (Art. 27) and **prior consultation** (Art 28) functions:[9]

> Art. 27
> Processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the European Data Protection Supervisor.
>
> Art. 28
> 1. The Community institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures relating to the processing of personal data involving a Community institution or body alone or jointly with others.
> 2. When it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.

Similarly, the Council Framework Decision 2008/977/JHA provides for **prior consultation**:

> Member States shall ensure that the competent national supervisory authorities are consulted prior to the processing of personal data which will form part of a new filing system to be created where:
> (a) special categories of data referred to in Article 6 are to be processed; or
> (b) the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.

3. PIA legal bases

No hard-law basis for PIA in the laws of European Union has been found.

However, there is a soft-law basis for PIA for RFID applications. In the constitutional system of the EU, a recommendation is a non-binding legal instrument.[10] The addressee of the recommendation is called on, but not placed under any legal obligation, to behave in a particular way. Pursuant to this provision, the 2009 **RFID Recommendation**[11] has set a legal basis for the RFID PIA Framework in the EU. The RFID PIA Framework is built upon it (see *infra*).

In addition, the European Commission has adopted a policy of conducting (regulatory) **impact assessment** (IA). Even though it consists only of a small privacy and data protection component (see *infra*), it is worth analysing briefly its legal framework.

[9] EDPS' opinions on prior checking are published online at: http://www.edps.europa.eu:80/EDPSWEB/edps/cache/off/Supervision/priorchecking and prior consultation opinions at http://www.edps.europa.eu:80/EDPSWEB/edps/cache/off/Consultation/OpinionsC
[10] *Cf.* Art. 288 TFEU, ex. Art. 249 TEC.
[11] European Commission, Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

This type of IA is to be applied to all sectors of the Commission's work in response to a mandate from the 2001 Gothenburg[12] and Laeken[13] European Councils (predominantly).[14] IA is an action of the Better Regulation Action Plan.[15] Since 2006, the Impact Assessment Board (IAB)[16] within the Commission's Secretariat-General examines and issues non-binding opinions on initiatives together with their IA reports. The Commission ultimately decides whether or not to adopt an initiative, taking account of the IA and the Board's opinion. The most recent IA guidelines come from 2009 (see *infra*).

In November 2005, the three EU institutions: the Commission, the Parliament and the Council have agreed on an inter-institutional common approach to IA.[17] In the legislative procedures of the EU, the Parliament and the Council have agreed to assess the impacts of their own substantive amendments to the Commission's proposal, and in doing so they will use the Commission's IA as the starting point for their further work. However, the legal status of inter-institutional agreements (IIAs) is unclear.[18]

Nevertheless, since 2010, when the Commission has adopted its new Rules of Procedure,[19] the IA is explicitly mandated:

> Article 23
> Cooperation and coordination between departments
>
> 4. The Legal Service shall be consulted on all drafts or proposals for legal instruments and on all documents which may have legal implications.
> 5. The Secretariat-General shall be consulted on all initiatives which:
> …
> – are subject to impact assessment or public consultation,
> and for any joint position or initiative that may commit the Commission vis-à-vis other institutions or bodies.

4. Guidance material

The landmark PIA guidance material in the EU is the **Radio-Frequency Identification (RFID) PIA framework**. In 2009, in the Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, the Commission stated (Art. 4):

[12] *Cf.* para 24 of the Presidency Conclusions. Göteborg European Council, 15-16 June 2001. http://ec.europa.eu/governance/impact/background/docs/goteborg_concl_en.pdf
[13] Presidency Conclusions. European Council Meeting In Laeken, 14-15 December 2001. http://ec.europa.eu/governance/impact/background/docs/laeken_concl_en.pdf
[14] Ruddy, T.F. and Hilty, L.M., "Impact assessment and policy learning in the European Commission", *Environmental Impact Assessment Review*, Vol. 28 No. 2-3, 2008, pp. 90-105. Further information on the history of Impact Assessment in the EU can be found there.
[15] European Commission, Communication from the Commission on impact assessment, COM(2002) 276 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0276:FIN:EN:PDF
[16] Impact Assessment Board, http://ec.europa.eu/governance/impact/iab/iab_en.htm
[17] Inter-Institutional Common Approach to Impact Assessment (IA). http://ec.europa.eu/governance/impact/ia_in_other/docs/ii_common_approach_to_ia_en.pdf
[18] Meuwese, A., *Impact Assessment in EU Lawmaking*, Ph.D. Thesis, Uni. Leiden, 2008, pp. 102-104. https://openaccess.leidenuniv.nl/bitstream/handle/1887/12589/Thesis.pdf?sequence=3
[19] Commission Decision of 24 February 2010 amending its Rules of Procedure (2010/138/EU, Euratom). These Rules are adopted pursuant to Art. 249(1) TFEU.

> Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union.

In the Recital 17 of the said Recommendation, the Commission explained:

> A framework developed at Community level for conducting privacy and data protection impact assessments will ensure that the provisions of this Recommendation are followed coherently across Member States. The development of such framework should build on existing practices and experiences gained in Member States, in third countries and in the work conducted by the European Network and Information Security Agency (ENISA).

Following the Commission's Recommendation, the industry and other relevant stakeholders prepared the RFID PIA framework. On 31 March 2010 they submitted it for endorsement by the Art. 29 Working Party. On 13 July 2010 the Working Party rejected it.[20] The revised Framework was submitted on 12 January 2011. On 11 February 2011 the Working Party finally endorsed the RFID PIA framework.[21]

The European Commission's internal Impact Assessment Guidelines require examining the impact of the proposed measure on certain considerations, which include privacy and data protection.[22] The Commission's **regulatory impact assessment** consists of three major steps (p. 31), of which the first one is the identification of economic, social and environmental impacts. For this step, the Guidelines advise to ask a number of key questions. Those regarding "*Individuals, private and family life, personal data*" are placed in Table 2 titled "*Social Impacts*" and include:

> Does the option impose additional administrative requirements on individuals or increase administrative complexity?
> Does the option affect the privacy, of individuals (including their home and communications)?
> Does it affect the right to liberty of individuals?
> Does it affect their right to move freely within the EU?
> Does it affect family life or the legal, economic or social protection of the family?
> Does it affect the rights of the child?
> Does the option involve the processing of personal data or the concerned individual's right of access to personal data?

5. Proposals

The plans for the revision of the EU data protection framework have been made public in November 2010 with the Commission's Communication "*A comprehensive approach on personal data protection in the European Union*". Pont 2.2.4 states, among others:

[20] Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf
[21] Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
[22] European Commission, *Impact Assessment Guidelines*, SEC(2009) 92.
http://ec.europa.eu/enterprise/policies/sme/files/docs/sba/iag_2009_en.pdf

> The Commission will examine the following elements to enhance data controllers' responsibility:
> …
> – including in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance

The European Parliament, in its resolution on passenger name records[23] (May 2010) called that:

> any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test.

COUNCIL OF EUROPE (COE)

1. General framework for privacy and data protection

The basic fundamental rights protection instrument is the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ECHR; ETS 5). Art. 8 provides for the right to respect for private and family life, home and correspondence. The ECHR establishes the European Court of Human Rights (ECtHR) in Strasbourg. Its landmark decisions in the field of privacy include e.g. *K.U. v. Finland* (2872/02) and *Von Hannover v. Germany* (59320/00).[24] All EU member states are also member states of the Council of Europe and are bound by the Convention. The EU itself it not yet bound by the Convention, but it is obliged to accede by virtue of Art. 6(2) of the TEU. Negotiations started in 2010.

All EU member states are bound by the CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). The EU accession is pending.[25] The Additional Protocol regarding supervisory authorities (ETS 181) binds the majority of EU member states and trans-border data flows.

2. Laws on PIA forerunners

Art. 1 of the Additional Protocol empowers national supervisory authorities with certain **investigation and intervention** functions:

[23] European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN

[24] See further e.g. Council of Europe, *Case Law of the European Court of Human Rights concerning the Protection of Personal Data*, 2009. http://www.data-protection-day.net/files/20101216_DP-(2009)-Case-Law_en.pdf.

[25] Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, approved by the Committee of Ministers, in Strasbourg, on 15 June 1999. http://conventions.coe.int/treaty/en/treaties/html/108-1.htm

> 1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol. ...
> 2.a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

Albeit it does not explicitly recall nor prior checking (consultation) nor PIA, the Explanatory Report to the said Protocol clarified that:[26]

> 13. The supervisory authority's power of intervention may take various forms in domestic law. … This power could also include the possibility to issue opinions prior to the implementation of data processing operations, or to refer cases to national parliaments or other state institutions. …
> 16. The supervisory authority's competences are not limited to the ones listed in Article 1 paragraph 2. It should be borne in mind that the Parties have other means of making the task of the supervisory authority effective. … The authority could be entitled to carry out prior checks on the legitimacy of data processing operations and to keep a data processing register open to the public. The authority could also be asked to give its opinion when legislative, regulatory or administrative measures concerning personal data processing are in preparation, or on codes of conduct.

3. Proposals

Some of Council's reports call for a PIA be introduced, *inter alia*:

- Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation (December 2010):[27]

> 4.3. The employer should take appropriate measures to assess the impact of any data processing which poses specific risks to the right to privacy, human dignity and protection of personal data, and to process such data in the least invasive manner possible. The agreement of employees or their representatives should be sought before the introduction or adaptation of such systems, programs or devices where the information or consultation procedure referred to in paragraph 4.2 reveals such risks unless domestic law or practice provides other appropriate safeguards.

- Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data (June 2011), overviewing results of consultation procedure:[28]

---

[26] Council of Europe, Directorate General of Human Rights and Legal Affairs, Data protection. Compilation of Council of Europe texts, Strasbourg, November 2010, p. 32.
http://www.coe.int/lportal/c/document_library/get_file?uuid=1d807537-6969-48e5-89f4-48e3a3140d75&groupId=10227

[27] Council of Europe, *Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation*, T-PD-BUR(2010)11.
http://www.coe.int/t/dghl/standardsetting/dataprotection/T-PD%20BUR(2010)11%20EN%20FINAL.pdf

[28] Council of Europe, *Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data*, T-PD-BUR(2011) 10 en.
http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD-BUR_2011_10_en.pdf

118. The Bulgarian Personal Data Protection Commission considers that, for this principle to be applied effectively, data controllers should be required to carry out assessments of the risk to privacy in data processing. Privacy International also favours an obligation to carry out a privacy impact assessment for major projects.

ANNEX 2 – LEGAL BASES FOR PIA IN BRITISH COLOMBIA AND OHIO

10.6 BRITISH COLOMBIA

1. PIA legal bases

Sec. 69 of the **Freedom of Information and Protection of Privacy Act (FOIPPA)**[29] explicitly provides for PIA be conducted:

> (1) In this section:
> …
> "privacy impact assessment" means an assessment that is conducted to determine if a new enactment, system, project or program meets the requirements of Part 3 of this Act.
> (5) The head of a ministry must conduct a privacy impact assessment and prepare an information-sharing agreement in accordance with the directions of the minister responsible for this Act.

2. Guidance material

The Office of the Chief Information Officer (OCIO) has issued PIA guidance[30] and template.[31]

10.7 OHIO

1. General framework for privacy and data protection

The Ohio Privacy Act is incorporated into Ch. 1347 of the **Ohio Revised Code**.[32] There is a State of Ohio Privacy and Security Information Center.[33]

2. Laws on PIA forerunners

Section 128.18(C) of the **Ohio Revised Code,** establishing the Office of Information Technology (OIT) within the Department of Administrative Services (DAS), provides for **privacy impact statement**:

> (1) The chief information security officer shall assist each state agency with the development of an information technology security strategic plan and review that plan, and each state agency shall submit that plan to the state chief information officer. The chief information security officer may require that each state agency update its information technology security strategic plan annually as determined by the state chief information officer.

---

[29] Freedom of Information and Protection of Privacy Act (FOIPPA), [RSBC 1996] Ch 165. http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

[30] Office of the Information and Privacy Commissioner for British Colombia, *Privacy Impact Assessment Process (PIA)*, [no date]. http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page

[31] Office of the Information and Privacy Commissioner for British Colombia, *Privacy Impact Assessment Process. PIA Template*, http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/pia_template.doc

[32] Cf. http://codes.ohio.gov/orc/1347

[33] State of Ohio Privacy & Security Information Center. http://www.privacy.ohio.gov

(2) Prior to the implementation of any information technology data system, a state agency shall prepare or have prepared a privacy impact statement for that system.

3. PIA legal bases

Section 1347.15 of the Code, dealing with confidential personal information,[34] provides for PIA be conducted:

(B) Each state agency shall adopt rules under Chapter 119. of the Revised Code regulating access to the confidential personal information the agency keeps, whether electronically or on paper. The rules shall include all the following:

….

(8) A requirement that the data privacy point of contact for the state agency complete a privacy impact assessment form.

Pursuant to section 1347.15(A)(1), "confidential personal information" means personal information that is not a public record for purposes of Sec. 149.43 of the Ohio Revised Code. This includes, among other things, medical data, certain DNA records or donor profile records.

4. Guidance material

In 2010, in order to comply with Sec. 1347.15 of the Code, the Office for Information Security and Privacy has issued a set of instructions[35] for PIA for existing personal information systems and a template[36] for these purposes.

[34] Cf. http://codes.ohio.gov/orc/1347.15
[35] Cf. http://www.privacy.ohio.gov/Government.aspx
[36] Cf. http://www.privacy.ohio.gov/resources/1347.15ImplementationPlanTemplate.doc