APPENDIX F

Privacy Impact Assessments
Jurisdictional Report for New Zealand

CONTENTS

Context

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

Legislative and Policy Framework

Legislation

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

In 1993, the *Privacy Act 1993* superseded the 1991 law.[1]

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

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

Public Sector Privacy Policy and Guidance Material

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

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

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

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

Key features of the Handbook are summarised in Appendix 1.

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

---

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

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

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

The New Zealand PIA Processes

History of the PIA in New Zealand

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

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

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

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

The Tools

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

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

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

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

Completion of PIAs

By Whom, When and under what circumstances?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Who participates?

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

External Consultation

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

Review/Approval of PIAs

Internal Review

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

Central Agency Review

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

Oversight Office Review and Acceptance

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

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

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

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

External Review

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

Public Availability

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

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

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

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

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

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

Other PIA Tools and Processes in New Zealand

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

PIA Template and Process Review and Revision

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

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

Review of PIA Policy/Legislation

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

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

Lessons Learned

Utility of PIAs in New Zealand

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

Room for Improvement

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

Oversight Body

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

Central Agency

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

Practitioners and the Public

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

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

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

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

No practitioners were interviewed during the course of the Study.

Research

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

Appendix 1: Key features of the PIA Handbook

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

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

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

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

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

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

   and (p. 6):

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

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

   and (p. 13):

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

   and (p. 29):

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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