Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The state of the art in privacy impact assessment

David Wright

Trilateral Research & Consulting, London, UK

Keywords:
Privacy impact assessment
PIAF
New data protection framework
Trust
Transparency
Stakeholder consultation
Threshold analysis

ABSTRACT

There is growing interest in Europe in privacy impact assessment (PIA). The UK introduced the first PIA methodology in Europe in 2007, and Ireland followed in 2010. PIAs provide a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments in the development of a new technology, service or product. This paper presents some findings from the Privacy Impact Assessment Framework (PIAF) project and, in particular, the project's first deliverable, which analyses the similarities and differences between PIA methodologies in Australia, Canada, Hong Kong, Ireland, New Zealand, the United Kingdom and the United States, with a view to picking out the best elements which could be used in constructing an optimised PIA methodology for Europe. The project, which began in January 2011, is being undertaken for the European Commission's Directorate General Justice. The first deliverable was completed in September. The paper provides some background on privacy impact assessment, identifies some of its benefits and discusses elements that can be used in construction of a state-of-the-art PIA methodology.

1. Introduction

The European Commission is expected to issue its proposed revisions to the data protection framework in early 2012. A draft of the proposed Data Protection Regulation was leaked in December 2011. It contains an article which makes a data protection impact assessment mandatory "where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes". The article sets out examples of such risks, which include "an evaluation of personal aspects relating to a natural person… information on sex life, health, race and ethnic origin… video surveillance… genetic data or biometric data… or other processing operations for which the consultation of the supervisory authority is required". The Commission had already announced its intention to make data protection impact assessments mandatory in its Communication of 4 November 2010.[1]

In January 2011, a year before the release of the draft Regulation, work began on the Privacy Impact Assessment Framework (PIAF) project, which is being undertaken for the Commission's Directorate General Justice by a consortium comprising Vrije Universiteit Brussel (VUB), Trilateral Research and Consulting, and Privacy International. The objective of the project is to provide a review and analysis of privacy impact assessment methodologies in Australia, Canada, Hong Kong, New Zealand, the UK and US and to make recommendations for an optimised privacy impact assessment framework for Europe, i.e., we aim to take the best elements of existing PIA policies and practices, and commend those to European policy-makers.

We have completed work on our first deliverable which can be found on the consortium's website.[2] The first

[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] http://www.piafproject.eu.

0267-3649/$ – see front matter © 2011 David Wright. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2011.11.007

deliverable reviews PIA policies and practices in the six above-mentioned countries plus Ireland as well as 10 case studies of PIA reports. The report also has a set of conclusions which identifies the benefits to organisations of undertaking privacy impact assessments and some of the best elements we have found in our review of existing policies and practices.

The PIAF report represents the state of the art in privacy impact assessment. To our knowledge, it is the most complete compendium and analysis of PIA methodologies, policies and practices yet compiled.

2. Definition

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. It is a process that should continue until and even after the project has been deployed.[3]

Although privacy impact assessment has been used in Australia, Canada, New Zealand and the United States since the mid-1990s, the methodology is a relatively new phenomenon in Europe. The UK Information Commissioner's Office published its PIA Handbook in December 2007 and a revised version in June 2009. It became the first country in Europe to publish a PIA guidance. Ireland became the second with the publication of its PIA guidance in December 2010.[4]

These two guidance documents, like those in Australia, Canada, New Zealand and the US, have some good points but also some shortcomings. Thus, Europe has the opportunity to build on the experience of others to develop a state-of-the-art PIA policy and practice. It can also take into account the RFID PIA Framework which was developed by some industry players and endorsed by the Article 29 Working Party in February 2011.[5]

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:

3. Benefits

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.[6]

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 can be a credible source of information. It enables an organisation to learn about the privacy pitfalls of a project directly, rather than having its critics or competitors point them out. A PIA assists in anticipating and responding to the public's privacy concerns.

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.[7]

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

[3] 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.

[4] 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.

[5] The PIAF project does not include a review of the RFID PIA Framework which was published several months after our consortium submitted its proposal to DG Justice. A copy of the revised RFID PIA Framework can be found here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf. The Art 29 Working Party's Opinion on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications can be found here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf.

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

[7] The organisation may not be able to eliminate privacy risks completely, despite its best efforts. Indeed, even after making some noble efforts, a company may decide the residual risk is worth accepting in view of the benefits the project may deliver – and these benefits might be not only to a company's bottom line, but also in a service that's genuinely valued by a wide swathe of society.

problems that might damage the organisation. It is a way to affirm the organisation's values. An organisation may wish to use a PIA as a way to check out third-party suppliers, to verify that they will not create privacy problems.

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. A PIA is a self- or co-regulatory instrument which may obviate the need for "hard" law, e.g., the RFID PIA Framework has (so far) obviated the need for specific regulation of RFIDs.[8] Thus, if organisations are seen to carry out proper (full-blooded) PIAs, they may escape the more onerous burdens imposed by legislation.

Some companies have given their own particular reasons for conducting privacy impact assessment. For example, Nokia has four main reasons for conducting privacy assessments:

1. to measure the implementation of privacy requirements, to get an understanding of the current status (risks, controls, root causes, etc.);
2. to find out if new projects follow privacy requirements;
3. to serve as a repository for information requests from authorities and consumers;
4. to improve general awareness.[9]

As another corporate example, Vodafone representatives have identified some further reasons for conducting a PIA:

- as an element of accountability, to demonstrate that the PIA process was performed appropriately;
- to provide a basis for post-implementation review;
- to provide a basis for audit, which is an objective and neutral assessment undertaken by a person or team who is *not* part of delivering the PIA;
- to provide "corporate memory", ensuring that the information gained during the project can be shared with future PIA teams and others outside the organisation.[10]

Corporate endorsements of PIA such as these may help their more timid peers to take a more dispassionate, objective look at the benefits rather than simply and thoughtlessly dismissing PIA as a hassle.

4. Elements in good policy and practice

The extent to which an organisation can achieve these and other benefits depends on the elements that go into the construction of a PIA policy and practice. From our review of PIA in the seven aforementioned countries, we have identified various elements that should be included in a PIA framework for Europe. Among them are the following:

4.1. *Roles – Who initiates a PIA and who approves it?*

A PIA policy should clarify who should initiate a PIA and who should approve it. Typically, responsibility for initiating the PIA should fall on the shoulders of the project manager. The organisation's privacy officer should provide guidance. The PIA should be signed off by a senior executive who is held accountable for its adequacy.

4.2. *Threshold analysis – Is a PIA necessary?*

An organisation should perform a preliminary threshold analysis of every project to determine whether a PIA is necessary. Threshold analyses typically consist of a set of questions to help uncover potential impacts. Many PIA methodologies include a threshold analysis.

4.3. *Clarify for whom the PIA is prepared*

Those undertaking a PIA should be clear for whom they are preparing it – e.g., for senior management, for the regulator, for stakeholders, for the public. As part of this, they should work from agreed (in writing) terms of reference.

4.4. *Process*

A PIA should be regarded as a process. It is not about preparing a report, although a report helps document the process. It is a process that should start when a project is in the early planning stages and should carry on throughout the project's life. New risks may emerge as the project progresses.

There are differences in PIA methodologies and processes, but one could formulate the main steps in the process as follows:

- Determining whether a PIA is necessary (threshold analysis)
- Identifying the PIA team and setting terms of reference
- Description of the proposed project and identification of stakeholders
- Analysis of the information flows and other privacy impacts
- Consultation with stakeholders
- Identification of risks and possible solutions
- Formulation of recommendations
- Preparation and publication of the report, e.g., on the organisation's website

[8] For more on the development of the RFID PIA Framework, see Spiekermann, Sarah, "The RFID PIA – developed by industry, endorsed by regulators" and Beslay, Laurent, and Ann-Christine Lacoste, "Double-take: getting to the RFID PIA Framework", both in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012. See also footnote [5] above. Beslay and Lacoste point out that PIA can be "used in two different contexts: in the first case, it represents a possible alternative to the adoption of a specific and binding regulation on RFID, while in the second case, it is part of the regulatory process, as a pre-condition to assess whether legislation is needed."

[9] Bräutigam, Tobias, Legal Counsel (Privacy), Nokia Corporation, "PIA: Cornerstone of privacy compliance in Nokia", in Wright and De Hert, op. cit.

[10] Deadman, Stephen, and Amanda Chandler, "Vodafone's approach to privacy impact assessments", in Wright and De Hert, op. cit. Deadman and Chandler are senior privacy officials at Vodafone Group.

- Implementation of the recommendations
- Third-party review and/or audit of the PIA
- Updating the PIA if there are changes in the project.

4.5. *Scale and scope of the PIA*

The scale and scope of a PIA should generally be in line with the scale and scope of a project. A more elaborate PIA – and more resources for carrying it out – will be needed for a complex project. A PIA should be conducted in a manner that is commensurate with the privacy risk identified. If the risks are not significant, then the scale and scope of a PIA could be limited. If the risks are significant, then the PIA should be more detailed. If the initial assessment reveals that there are significant risks, then the project manager should involve stakeholders to help in considering those and any other risks that may become apparent in the course of the PIA.

The Victoria Privacy Commissioner's PIA Guide rightly notes that "the size or budget for a project is not a useful indicator of its likely impact on privacy".[11] The UK ICO PIA Handbook distinguishes between full-scale and small-scale PIAs.[12] According to the ICO, the phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalised and does not warrant as great an investment of time and resources in analysis and information-gathering.

The distinction between a full-scale and small-scale PIA seems artificial. Where would one draw the border between the two? The scale and scope of PIA should reflect the complexity and significance of the perceived privacy risks.

In some instances, generic PIAs may be justifiable where an organisation undertakes similar projects or applications.[13]

4.6. *PIA starts early*

The sooner a PIA starts the better. It should start early enough so that it can influence the design of a project. It is useless if it is undertaken after all the decisions have been made. Unlike other PIA methodologies that say PIAs should be initiated as early as possible, the Office of the Information and Privacy Commissioner (OIPC) in Alberta says in its PIA Requirements 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.[14] 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.

4.7. *Privacy, not just data protection*

The European Commission has used the term "data protection impact assessment", a term of more limited scope than a "privacy impact assessment". PIA is the terminology that has been used by all other countries, and we think that using the term DPIA risks sending the wrong message to organisations. Informational privacy is only one type of privacy, as the Australian PIA Guide (at p. iii) and some of its counterparts note. The ICO Handbook distinguishes four "aspects" of privacy, i.e., privacy of personal information, privacy of the person; privacy of personal behaviour; and privacy of personal communications.[15] (The last privacy frontier might be privacy of thought and feelings.) If industry and governments think the Commission's main or only concern is with data protection (information privacy), then these other forms of privacy could be brushed aside.

4.8. *PIA as part of risk management*

Most PIA guidance documents say that PIA should be viewed as part of an organisation's risk management practice. We agree. PIAs are about identifying risks and finding solutions. They should not be seen as somehow distinct from risk management, as simply a compliance check.

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

[11] Office of the Victorian Privacy Commissioner (OVPC), *Privacy Impact Assessments: A guide for the Victorian Public Sector*, Edition 2, April 2009, p. 5. http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/publication-types?opendocument&Subcategory=Guidelines&s=.

[12] Information Commissioner's Office (ICO), *Privacy Impact Assessment Handbook*, Version 2.0, Wilmslow, Cheshire, June 2009. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx.

[13] Canada's Privacy Commissioner, as an example, has referred to the possibility of generic PIAs: "In other cases, as with shared services or system initiatives where entities use the same or similar approaches to the collection, use and disclosure of personal information, generic assessments might be better employed." See Stoddart, Jennifer, "Auditing privacy impact assessments: the Canadian experience", in Wright and De Hert, op. cit.

[14] Office of the Information and Privacy Commissioner (OIPC) of Alberta, *Privacy Impact Assessment (PIA) Requirements For use with the Health Information Act*, January 2009, p. 13. www.OIPC.ab.ca.

[15] ICO Handbook, op. cit., 2009, p. 14. Roger Clarke distinguished these different dimensions (or types) of privacy some years ago. See Clarke, Roger, "What's privacy?", 2006. http://www.rogerclarke.com/DV/Privacy.html.

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).

4.9. *Questions to identify risks and solutions*

Almost all PIA guidance documents contain a set of questions to help project managers and those carrying out PIAs to identify privacy risks. Sometimes, these questions relate to privacy principles. Usually, the questions require more than a yes or no response; respondents must provide some details to support their yes or no. The responses to the questions often serve as the basis of the privacy impact assessment report.

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 included in most PIA guidance documents can help stimulate consideration of possible privacy impacts.

4.10. *PIAs are only as good as the processes that support them*

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.

In its audit of PIAs undertaken in the Canadian government, the Office of the Privacy Commissioner (OPC) commented that how an organisation complies with the government's PIA policy presupposes the existence of some administrative structure to support the policy's objectives and requirements. The OPC said key elements of a sound infrastructure should include:

- Programs in place to inform staff and other stakeholders of the policy's objectives and requirements;
- Formally defined program responsibilities and accountabilities;
- The existence of a system to effectively report all new initiatives that may require a PIA;
- The existence of a body composed of senior personnel charged with reviewing and approving PIA candidates;
- The existence of an effective system of monitoring compliance with the PIA policy;
- Adequate resources committed to support the organisation's obligations under the policy.[16]

4.11. *Training and raising awareness of employees*

Coupled with the above, and to embed PIA within its culture and practices, the organisation needs to install an ongoing employee awareness program, effectively raising the profile of PIAs and regulatory requirements for their performance with program managers and new hires. Creating general awareness of the policy requirements respecting privacy is often the first step towards ensuring that program managers fully consider the privacy impacts of their plans and priorities at the time an initiative is conceived.[17]

4.12. *Mandatory PIAs*

Undoubtedly, a contentious issue is whether PIAs should be mandatory, as the European Commission indicates in its draft Regulation. PIA is already mandatory in Canada, the UK and the US, at least for government agencies. They are also mandatory for the private sector in certain other instances, for example, involving health care (e.g., in Alberta[18]) or biometrics (New Zealand[19]). There is a strong case for mandatory PIA, as the Commission indicates, in projects involving sensitive data, surveillance and profiling. Unless they are mandatory, many organisations may not undertake them even though their projects, technologies or services have serious privacy impacts. Nevertheless, the logistics of mandatory PIA are not so straightforward. Mandatory PIA would need to be complemented by audits and, desirably, publication and stakeholder engagement.[20]

4.13. *Engaging stakeholders*

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. Engaging stakeholders is a way of testing the waters, of gauging the public's reaction to a project before it is implemented.

[16] Office of the Privacy Commissioner of Canada (OPC), *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report of the Privacy Commissioner of Canada, Ottawa, 2007, p. 9.

[17] Ibid., p. 17.

[18] Section 64 of Alberta's Health Information Act 2000 says "(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)." http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest.

[19] Section 32 of the NZ Immigration Act 2009 explicitly requires that a PIA be conducted if biometric information is processed. It requires PIAs regarding the collection and processing of biometric data to be published on the department's website. See Immigration Act 2009, Public Act 2009 No 51. http://www.legislation.govt.nz/act/public/2009/0051/latest/096be8ed806837b3.pdf.

[20] For more on this issue, see Wright, David, "Should privacy impact assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011. http://cacm.acm.org/magazines/2011/8.

Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report.

The ICO PIA Handbook puts a strong emphasis on stakeholder engagement and consultation. The ICO says that if a PIA is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It therefore recommends that stakeholder perspectives are considered.[21] Australia's PIA Guide makes a similar point. It says "Consultation with key stakeholders is basic to the PIA process." It adds that:

> *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.*

PIA expert Roger Clarke describes consultation as central to the PIA 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."[22]

In this context, one should recall Article 41 of the Charter of Fundamental Rights of the European Union, entitled "The right to good administration" – i.e., this right includes "the right of every person to be heard, before any individual measure which would affect him or her adversely is taken", which suggests that consultation with stakeholders is not only desirable but necessary. Even if consultation does not increase support for a decision, it may clear up misunderstandings about the project and, at least, gain the respect of stakeholders.

Consultation will be most effective when the stakeholders consulted are representative of those interested in or affected by a project. If an organisation tries to "fix" a consultation by consulting only "safe" stakeholders, those that will go along with its point of view, it actually does itself a disservice, not just by making a sham of the process, but also by not achieving the advantages and benefits of a consultation which is aimed at identifying risks, obtaining fresh information and finding solutions, in other words of achieving a "win–win" result so that everyone benefits.

4.14. *Recommendations and an action plan*

It is not sufficient for a PIA report to simply make a set of recommendations. An action plan is needed to ensure those recommendations are implemented or, if not, some explanation given as to why some recommendations are not implemented. If PIA is viewed as a process, then the process should continue after preparation of the PIA report to ensure recommendations are implemented.

4.15. *Publication of the PIA report*

A PIA report should normally be publicly available and posted on an organisation's website so as to increase transparency and inspire public confidence.

Under the US E-Government Act of 2002, government agencies are obliged to publish their PIA reports unless it is necessary to protect classified, sensitive or private information contained in the assessment. Even with such exceptions, the organisation could redact the sensitive information and publish the report – or put the sensitive information in a confidential appendix, as the ICO Handbook suggests.[23] In Canada, agencies are obliged to publish somewhat detailed summaries, but publication of the full report is obviously better, as it will instil greater confidence that the organisation has identified the privacy risks and is adopting measures to counter those risks. Publication of the report creates another opportunity for gathering stakeholder views.

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.

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.

4.16. *PIAs, state security and commercially sensitive issues*

State security and commercially sensitive information need not – should not – be legitimate reasons for not conducting a PIA. Where there are legitimate concerns about making those PIAs public, ways can usually be found to deal with the concerns – for example, through redaction of sensitive information, third-party audit, oversight by the data

[21] ICO, PIA Handbook, p. 56, p. 58.

[22] Clarke Roger, "PIAs in Australia: A work-in-progress report", in Wright and De Hert, op. cit. Clarke cites his earlier article: "Privacy Impact Assessment Guidelines", Xamax Consultancy Pty Ltd, February 1998. http://www.xamax.com.au/DV/PIA.html.

[23] "Where some of the information is subject to commercial or security sensitivity, that information can be separated into an appendix, which can be distributed less widely and/or subject to clear confidentiality constraints.... There may be resistance within the organisation to providing some of this information to stakeholders.... On the other hand stakeholder trust needs to be achieved." ICO, PIA Handbook, op. cit., pp. 33–34.

protection authority and the engagement of external stakeholders through non-disclosure agreements. Generally, however, 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. Even the US Department of Homeland Security has recognised this, saying: "A PIA should be conducted for *all* systems handling personally identifiable information *including classified or law enforcement sensitive programs*."[24] [Italics added.]

4.17. *Monitoring implementation of recommendations and third-party audits*

In the first instance, the organisation itself is responsible for implementing the recommendations (at least, those with which it agrees). In some instances, the data protection authorities or privacy commissioners may need to monitor implementation. Third-party audits, such as those performed by the Government Accountability Office (GAO) in the US and the Office of the Privacy Commissioner in Canada, show the utility of audits, including from the perspective of the organisation itself. Audits lead to improvements in PIA practice.

A third-party review and/or audit of PIAs is necessary, as Nigel Waters points out, because it is all too easy for project proponents to say initially that they accept and will implement suggested changes, only to find reasons later to backslide, and either partially or wholly abandon their initial commitment.[25]

It seems desirable for organisations, from both the public and private sectors, to send copies of their PIA reports to the data protection authority (DPA or privacy commissioner, as the case may be). Such a practice would be somewhat similar to the obligation in many Member States whereby an organisation must check with the DPA before compiling and processing a database of personal data (a consequence of Art. 20 on prior checking of the EU Data Protection Directive[26]). The DPA will not have the resources to review all of the PIAs, but it could perhaps undertake a random review of some of them (say 10 per cent). Sending PIA reports to the DPA could have several salutary consequences. One is that the organisation is more likely to take the time to prepare a proper PIA especially if it thinks that it might be that "one-in-10" that gets reviewed. Another is that the DPA will learn what makes an effective PIA and will be able to pass on "good practice" to all PIA assessors. A third is that the DPA will be able to judge whether organisations are becoming more concerned – or more careless – about privacy practices.

One could contemplate a kind of reward for an organisation whose PIA report has been subject to a third-party review or audit, e.g., a privacy seal that provides evidence of good practice.

4.18. *Cross-jurisdictional projects*

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.

So far, there are few instances of multi-agency or transnational PIAs. Yet projects or data exchanges between different organisations, including those based in different countries, may also have privacy impacts. Examples abound. US access to European passenger name records (PNRs) is one such. While a transnational PIA might be problematic on procedural and organisational terms, New Zealand's *Privacy Impact Assessment Handbook* foresaw some years ago that:

> *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.*[27]

The message here is that transnational projects should not escape the scrutiny of a PIA, simply because they are transnational. Mechanisms and procedures can be developed to deal with such projects – even if that has not happened yet.

Transnational PIA has attracted some attention in the corporate world. The international consultancy Deloitte & Touche published a guide to cross-border privacy impact assessment as long ago as 2001,[28] although aimed at companies with cross-border operations rather than government agencies. More recently, a PIA has been performed for a transnational medical information project in Europe.[29] Canada's national police force, the RCMP, has also participated in multi-agency PIAs including multilateral information agreements regarding immigrants.

[24] Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance*, Washington, DC, June 2010, p. 7. http://www.dhs.gov/files/publications/gc_1209396374339.shtm.

[25] Waters, Nigel, "Privacy impact assessment – Great potential not often realised", in Wright and De Hert, op. cit.

[26] Art. 20 says in part that "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."

[27] Stewart, Blair, *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, June 2007, p. 14. http://privacy.org.nz/privacy-impact-assessment-handbook/.

[28] Karol, Thomas J., *A Guide To Cross-Border Privacy Impact Assessments*, Deloitte & Touche, 2001. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/A-Guide-To-Cross-Border-Privacy-Impact-Assessments.aspx.

[29] Di Iorio, C.T., F. Carinci, J. Azzopardi et al., "Privacy impact assessment in the design of transnational public health information systems: the BIRO project", *Journal of Medical Ethics*, Vol. 35, 2009, pp. 753–761. http://jme.bmj.com/content/35/12/753.abstract.

4.19. *Accountability*

Accountability is a necessary condition of a successful PIA policy. A senior executive at board level, if not the chief executive officer, should be held accountable for the quality and adequacy of a PIA.

Accountability can arise from a requirement that a completed PIA be included in program and funding approval processes. Accountability for PIA completion can also be enhanced by mandatory reporting requirements. Notification and public disclosure are important instruments of accountability to the public. A senior executive at the board level should be accountable for the adequacy of a PIA.

4.20. *Tying PIAs to budget submissions*

In Canada and the US, PIAs are tied to budget submissions. In Canada, government institutions must complete and forward a PIA to the Treasury Board of Canada Secretariat to accompany submissions for funding new programs and projects, and in the US, government agencies must include a PIA with submissions to the Office of Management Budget. These are good practices to ensure that organisations actually do perform a PIA when undertaking an initiative with privacy impacts. It is another way to shore up accountability.

4.21. *A central registry of PIAs*

One of the recommendations from the audit done by the Privacy Commissioner of Canada is that the government should create a central registry for PIA summaries, as has been done in British Colombia and Alberta. This too is a good practice. It helps create a body of knowledge so that project managers and assessors can learn from the experience of others. It is also useful for greater transparency and for simplifying the search process.

Specifically, Privacy Commissioner Jennifer Stoddart is of the view that a central database or registry of PIAs would "provide a single window of access to PIAs (and thus privacy intrusive projects) across government, regardless of the originating department and program authority. The registry could be used by the public to better understand the substance of government projects and by central agencies such as the Treasury Board Secretariat and the Privacy Commissioner to monitor PIA activities." She says that a registry might also enhance the project management capabilities of institutions and facilitate knowledge sharing between government departments.[30]

5. Conclusion

Our review of PIA methodologies and reports show that there are similarities as well as differences in privacy impact assessment policies among the seven countries – Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and the US. Europe can benefit from their experience by drawing upon their best elements to create its own state-of-the-art PIA policy and practice. This paper has presented some of the elements that can be used to construct an optimised PIA. As the European Commission has already made provision for mandatory PIA (or data protection impact assessment) in the proposed Regulation, it is not too early for policy-makers, organisations, civil society organisations, privacy advocates and others to discuss the elements of an optimised, state-of-the-art PIA able to deliver the potential and benefits outlined early in this paper.

Acknowledgement

This paper is based on research partly supported by a project funded by the European Commission's Directorate General Justice under its Fundamental Rights & Citizenship Programme (Grant Agreement No. JUST/2010/FRAC/AG/1137 – 30-CE-0377117/00-70). The views expressed are those of the author alone and are not intended to reflect those of the Commission nor those of the PIAF consortium. The author presented an early version of this paper at the International Data Protection Conference, held in Warsaw 21 September 2011.

David Wright (david.wright@trilateralresearch.com) *is Managing Partner of Trilateral Research & Consulting, London. He is co-editor, with Paul De Hert, of Privacy Impact Assessment, Springer, Dordrecht, 2012.*

[30] Stoddart, Jennifer, "Auditing Privacy Impact Assessments: The Canadian Experience" in Wright and De Hert, op. cit.