Journal of Contemporary European Research

Volume 9, Issue 1 (2013)

A Comparative Analysis of Privacy Impact Assessment in Six Countries

David Wright *Trilateral Research*

Rachel Finn *Trilateral Research*

Rowena Rodrigues *Trilateral Research*

Citation

Wright, D., Finn, R. and Rodrigues, R. (2013). 'A Comparative Analysis of Privacy Impact Assessment in Six Countries'*, Journal of Contemporary European Research*. 9 (1), pp. 160-180.

First published at: www.jcer.net

Abstract

The European Commission is revising the EU's data protection framework. One of the changes concerns privacy impact assessment (PIA). This paper argues that the European Commission and the EU Member States should draw on the experience of other countries that have adopted PIA policies and methodologies to construct its own framework. There are similarities and differences in the approaches of Australia, Canada, Ireland, New Zealand, the UK and US, the countries with the most experience in PIA. Each has its strong points, but also shortcomings. Audits have identified some of the latter in the instance of Canada. This paper provides a comparative analysis of the six countries to identify some of the best elements that could be used to improve Article 33 in European Commission's proposed Data Protection Regulation.

Keywords

Privacy impact assessment, data protection impact assessment, compliance check, stakeholder consultation, risk management, Data Protection Regulation

---

The European Commission has proposed a major revision to the European Union's data protection framework. The proposed Regulation, released on 25 January 2012, represents the biggest overhaul in data protection since the Data Protection Directive (95/46/EC) was adopted in 1995. Article 33 of the proposed Regulation obliges organisations to conduct a 'data protection impact assessment' where processing operations present specific risks to the rights and freedoms of data subjects (European Commission, 2012). The Commission had already signalled its interest in privacy impact assessment (PIA) as an important instrument in the data protection toolkit well before publication of the proposed Regulation. For example, the Commission issued a Recommendation in May 2009 in which it said that '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' (European Commission, 2009). Although the Art. 29 WP rejected industry's first attempt, it did endorse a revised framework in February 2011. In its endorsement, the Art. 29 WP said that risk management 'is an essential component of any Privacy and Data Protection Impact Assessment Framework' (Art 29 WP, 2011). It also welcomed 'the explicit inclusion of a stakeholder consultation process as part of the internal procedures needed to support the execution of a PIA'. The Art. 29 WP concluded its Opinion with the observation that 'A PIA is a tool designed to promote 'privacy by design', better information to individuals as well as transparency and dialogue with competent authorities.'

A further example of the EC's interest in PIA was its co-funding the PIAF project[1], which was carried out by a consortium of Vrije Universiteit Brussel, Trilateral Research & Consulting and Privacy International. PIAF is the acronym for a Privacy Impact Assessment Framework. The 22-month project began in January 2011 and finished in October 2012. It reviewed existing PIA methodologies in those countries with the most experience in PIA, i.e., Australia, Canada, Ireland, New Zealand, the UK and the US.

This paper draws on the research undertaken in the PIAF project as well as other PIA-related sources to provide a comparative analysis against 18 benchmarks of privacy impact assessment policies and methodologies used in the above-mentioned countries. Among the benchmarks or points of comparison are whether PIAs are mandatory, whether they are to be published, whether they deal with just data protection (information privacy) or include other types of privacy within their scope, whether they

support consultation with stakeholders, whether they provide for third-party review or audit, and so on. Our paper breaks new ground by providing a comparative analysis of the key features of the PIA policies and methodologies in each country in order to make recommendations for construction of an optimised PIA policy and methodology for use within EU Member States (and elsewhere) based on the best elements of existing policies and recommendations.

LEARNING FROM THE EXPERIENCE OF OTHERS

Although there are differences between the PIA policies and methodologies in the six above-mentioned countries, one can also see an increasing convergence in approaches, in good part because later countries, the UK and Ireland, have sought to learn from the experience of others. The increasing convergence is manifested by, for example, the emphasis on stakeholder consultation which features strongly in the UK and Irish PIA guidance documents, but less so or not at all in some of their antecedents. Convergence is also seen in definitions too, for example, of the term "project". Even certain phrases (PIA is described as "an early warning system") turn up again and again.

In this paper, we define PIA as a methodology for assessing the impacts on privacy of a project, technology, product, service, policy, programme 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 deployment of the project.

While we discuss "privacy impact assessment" throughout this paper, the reader may wish to note that the European Commission has devised the terminology "data protection impact assessment". In its RFID Recommendation, it refers to "privacy and data protection impact assessment" (European Commission, 2009). We prefer the original term of privacy impact assessment, because we view data protection (information privacy) as only one type of privacy, and government agencies and companies should consider as well the risks to other types of privacy in any initiative they develop. Roger Clarke (1997, 2006) has identified four types (dimensions is the word he uses) of privacy – privacy of the person, of personal behaviour, of personal communications and of personal data.[2] All types of privacy should be taken into account in a privacy impact assessment. A data protection impact assessment is too limited in scope.

Paul De Hert (2012: 34) has criticized data protection impact assessment as merely a compliance check, 'simply checking the legal requirements spelled out in the European data protection framework'. He points out (De Hert, 2012: 33) that the Charter of Fundamental Rights of the European Union differentiates between privacy (Art. 7) and data protection (Art. 8). 'Depending on the nature of the data used, personal data and/or location data and/or traffic data, and depending on the nature of the processing involved (private, public, law enforcement), one can establish a checklist based on these regulations that when carried out properly will make up the data protection impact assessments. No more and no less (De Hert, 2012: 35). He goes on to argue that 'Beyond compliance checks with legal regulations, one must consider more qualitative requirements that have to do with legality, legitimacy, participation and, especially, proportionality… These qualitative principles – accounting for the difference between a compliance check and a true impact assessment – are key considerations in determining whether privacy is respected in the context of the ECHR [European Convention on Human Rights] and the relevant case law of the ECtHR [European Court of Human Rights] (De Hert, 2012: 38). Like Clarke, De Hert finds that privacy goes beyond data protection: 'the privacy right has served as a catch-all tool, covering a sophisticated collection of interests, ranging from intimacy, sexual choice, personal identity, moral and

physical well-being, reputation, formation of human relationships, health and environmental protection, collection of and access to personal information (De Hert, 2012: 39). For these and other reasons, we prefer the term privacy impact assessment over data protection impact assessment. The former is wider-ranging and can catch intrusions and compromises that may not be caught by a data protection impact assessment.

WHAT MAKES A GOOD PIA?

While the PIA literature is not voluminous (but is growing), researchers have identified criteria that make a "good" PIA. These include what a PIA is, how it should be conducted, what it should contain and how organisations undertaking PIAs should be supported, and how PIA recommendations should be implemented and monitored.

Roger Clarke (2011) and Colin Bennett (2007) argue that a PIA must be more than a compliance check with relevant privacy and data protection legislation. Experts agree that PIAs are especially effective if they are "pre-decisional", i.e., published before a system design or regulatory process is completed (Dempsey, 2004), which Bennett (2007: 13) argues allows for a significant amount of internal review and analysis before a technology or system is implemented. PIAs should also be regarded as a process that continues alongside the development of a project (Dempsey, 2004). PIAs should be regularly reviewed and may need to be updated if the technology or system is altered in any way. As such, a PIA should be understood as a "living" document, not a task which has been completed. Given these issues, we identify the following criteria against which to analyse PIA processes in the six countries. A PIA should:

- Be more than a compliance check;
- Be a process;
- Be reviewed, updated and on-going throughout the life a project.

Regarding how a PIA should be conducted, PIA experts regard stakeholder consultation as a key issue. Kenneth A. Bamberger and Deirdre K. Mulligan (2008) argue that consultation with a range of different stakeholders is one of the key ways in which privacy issues are identified and possible solutions are reviewed. According to these authors (2008: 87), 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'. As a result, a PIA should integrate consultation with external stakeholders.

Experts have also agreed that a PIA should be a forum for the identification of problems *and* solutions. A PIA should identify risks to privacy as well as information about how those risks can be mitigated (Rotenberg, 2006: 24-25). Rotenberg further 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. Furthermore, as noted above, "privacy", as a concept, includes a number of different facets or dimensions or types, and as such, a PIA should identify privacy risks associated with each type of privacy, not only information privacy or data protection. PIAs should also have the potential to 'avoid, mitigate, stop or suggest alternative solutions to privacy risks, as well as the ability to modify plans accordingly' (Tancock et al., 2010: 120). As such, a PIA should:

- Identify privacy risks;
- Address all types of privacy;
- Identify possible strategies for mitigating privacy risks.

Clarke (2009) argues that guidelines for conducting a PIA, including suggestions for how the report ought to be structured and what information it ought to include, should be established and made publicly available. Organisations should also be assisted in

understanding that a PIA is good business practice and part of an effective risk management strategy (Tancock et al., 2010). This could lead to increases in public trust and corporate reputation. In relation to their review of PIAs in US government agencies, Bamberger and Mulligan (2012) also find that the creation of an external oversight structure for the conduct of PIAs and a chief privacy officer within the organisation to oversee and approve the PIA both contributed to the successful implementation of PIAs in that sector. Consequently, an effective PIA depends upon the provision of:

- A suggested structure for the PIA report;
- An encouragement to publish the PIA report;
- An encouragement to have PIA reports signed off by senior management (to foster accountability);
- A policy that provides for third-party, independent review or audit of the completed PIA document.

We use these benchmarks to assess the PIA policies and methodologies in the six countries with the most PIA experience. We also actively seek out examples of best practice in addition to the guidelines mentioned above to construct an optimal PIA methodology for Europe.

Australia

We begin our review of PIA methodologies with Australia and, in particular, two guidance documents, one produced by the Office of the Privacy Commissioner of Australia and the other produced by the Office of the Privacy Commissioner of Victoria.

Office of the Privacy Commissioner of Australia

The Office of the Privacy Commissioner (OPC) published its *Privacy Impact Assessment Guide* in August 2006, and a revised version in May 2010. The *Guide* is addressed to those who undertake a PIA, irrespective of 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.

The Australian PIA Guide makes the point (at p. iii) that information privacy is only one aspect of privacy. Other types of privacy include privacy of the body, privacy of behaviour, privacy of location and privacy of communications, as mentioned above. It defines a project as 'any proposal, review, system, database, program, application, service or initiative that includes handling of personal information'.[3] 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).[4] 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'.

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;
2. Mapping the information flows and privacy framework;
3. Privacy impact analysis;
4. Privacy management;
5. Recommendations.

The *PIA Guide* (p. xix) says the Office of the Privacy Commissioner 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.

Victoria 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' (Clarke, 2012: 139). 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 (at 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*. It says the size or budget for a project is not a useful indicator of its likely impact on privacy. The *Guide* recommends that a simple threshold privacy assessment be routinely conducted for every project to determine whether a PIA is necessary. The *Guide* has 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 (at 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: releasing the report gives the public an opportunity to express concerns and have them addressed before a project has been implemented. The *Guide* says the PIA should be dynamic, updated as changes are contemplated to projects.

Organisations 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.

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' (OPC, 2007: 24).

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.

The *Guide* (at p. 20) generally recommends publication of the report, but recognizes some considerations, such as security, may influence the decision to publish. In such cases, it says that a properly edited PIA report would 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.

Canada

In Canada, policy responsibility for privacy impact assessment in the federal government lies with the Treasury Board of Canada Secretariat (TBS, 2008), which defines PIA as "a policy process for identifying, assessing and mitigating privacy risks". TBS promulgated a new Directive on Privacy Impact Assessment in April 2010. 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. 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, i.e., an overview and PIA "initiation", and specified "risk area identification and categorisation". 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' (TBS, 2008, 6.3.3).

The TBS does not approve PIAs; it only reviews them to ensure that the assessment is complete (TBS, 2010, 8.1.1). The TBS requirements put the emphasis 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[5]. While the directive does not refer to the TBS's PIA Guidelines, these are still recommended even if they have not been revised since August 2002.

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. These questions are somewhat like those in the privacy threshold assessment used in the Australian OPC 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*[6] as well as federal privacy legislation and policies.

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' (TBS, 2002, 2). The Guidelines identify several common privacy risks, such as data profiling/data matching, transaction monitoring, identification of individuals, physical observation of individuals, publishing or re-distribution of public databases containing personal information and lack or doubtful legal authority.

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

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 its PIA template and guidelines (OIPC, 2009). Those submitting PIAs are advised to consider the feedback from the OIPC before they implement their projects covered by Alberta's Health Information Act (HIA). 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' (OIPC, 2009: 5). The OIPC appears to exercise much more power than most of its counterparts. Not only are PIAs dealing with health information 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 than many of its counterparts elsewhere.

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" of health information 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.

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 at which 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. 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. 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.

Ireland

The Health Information and Quality Authority (HIQA) produced a PIA Guidance (HIQA, 2010b) following its review of PIA practice in other jurisdictions (HIQA, 2010a), 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. The PIA process involves evaluation of the 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. It says that a PIA in its own right may not highlight all privacy risks or issues associated with an initiative. A PIA is a tool; it depends on service providers' having the correct processes in place to carry out the PIA. These include identification of the 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.

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.

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 Guidance says 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.

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 published and presented in a reader-friendly format.

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 to undertake Information Matching Privacy Impact Assessments (IMPIAs).[7] 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 (OPC, 2010). The Office of the Privacy Commissioner (OPC) issued guidance on their implementation in 1999 (OPC, 2008).

The OPC (2007) published a *PIA Handbook* in October 2002 (reprinted in 2007). The *Handbook* defines a PIA as a 'systematic process for evaluating a proposal in terms of its impact upon privacy' (2007: 5), 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' (2007: 3).

The *Handbook* is useful for 'projects with a technological component, especially e-commerce and e-government initiatives', though it also aims to help businesses, government departments and others operating offline. According to the *Handbook* (2007: 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. The *Handbook* offers (2007: 21-28) in-depth practical advice on how to prepare privacy impact reports.

The *Handbook* outlines 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 them out) 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. (*Handbook*, 2007: 11)

The *Handbook* recommends (2007: 14) minimizing the duplication of PIA efforts by undertaking generic or overarching PIAs where planned projects are similar. The *Handbook* suggests (2007: 21) the following contents 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 *Handbook* outlines the following risks:

- Failing to comply with either the letter or the spirit of the 1993 Privacy Act, 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* recommends (2007: 21) that the PIA report is best written with a non-technical audience in mind and that it be made publicly available (2007: 19) (either in full or summary on an organisation's website). The *Handbook* mentions consultation with stakeholders (2007: 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 explicitly requires that PIA be conducted if biometric information is processed.

John Edwards, a PIA practitioner in New Zealand, 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' (Edwards, 2012: 198).

UK

The Information Commissioner's Office (ICO) commissioned a team of experts, coordinated 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 (ICO, 2007a). That same year, the ICO published a *PIA Handbook* (ICO, 2007b) making the UK the first country in Europe to do so. The ICO published a revised version in June 2009. 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.'[8]

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' (Cabinet Office, 2008a: 18). 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' (Cabinet Office, 2008b: Section I, 4.4).

The ICO (2009: 3) envisages a PIA as a process, separate from 'compliance checking or data protection audit processes', that should be undertaken when it can 'genuinely affect the development of a project'. (The *Handbook* uses the term "project" as a catch-all; 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' (2009: 2).

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.

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. It sets out 15 questions to help determine which is appropriate for a given project.

Warren and Charlesworth (2012) contend that there are several problems with the UK PIA system, one of which is the lack of review and oversight. 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. 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 further 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[9]; 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.

USA

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' (DHS, 2007: 8). The processing of PII in the US is also covered by Fair Information Practice Principles (FIPP) from the Privacy Act of 1974.

Section 208 of the E-Government Act requires that PIAs be reviewed by a chief information officer or equivalent, 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.

Roger Clarke (2009: 128) argues that some organisations are seeking to 'forestall legislative provisions' for PIAs by creating and supporting industry standards. Clarke argues that 'these processes have lacked the least vestige of consultation with people, or with their representatives or advocates for their interests.' He 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 the design of business systems. This is of considerable significance internationally, because US corporations have such substantial impact throughout the world. (Clarke, 2009: 128).

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 (OMB, 2003). 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.[10] 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 (OMB, 2003: Attachment A).

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. 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 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.

Table 1: Principal Similarities and Differences between the Different PIA Guidance Documents

Features The PIA guide…	**Australia**		**Canada**		**IE**	**NZ**	**UK**	**USA**
	National	Victoria	National	Alberta				OMB
Reviewed here, was published in	May 2010	Apr 2009	Aug 2002	Jan 2009	Dec 2010	Oct 2002 to 2007	Jun 2009	Sep 2003
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	✓	✓		✓	✓	✓	✓	✓
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).		✓	✓	✓	✓			✓

A COMPARISON OF PIA POLICIES AND METHODOLOGIES IN THE SURVEYED COUNTRIES

Table 1 identifies the principal similarities and differences between the different PIA guidance documents analysed in this paper based on the recommendations that make a "good" PIA. In addition to the recommendations discussed above, our review has also identified other best practice elements that we feel a successful PIA methodology or policy should include. It should also:

- Contain a set of questions to uncover privacy risks (usually in relation to privacy principles);
- Target companies as well as government departments;
- Regard PIA as a form of risk management;
- Identify benefits of undertaking a PIA;
- Provide a privacy threshold assessment to determine whether a PIA is necessary;
- Define "project" as including legislation and/or policy;
- Mandate the PIA by law, government policy or as an accompaniment to budget submissions.

Best elements

From our review and analysis of the above-referenced PIA methodologies, we have identified elements (practices) that could be used to construct a state-of-the-art European PIA policy and methodology. Following the structure of the discussion of "good" PIA criteria above, this section categorizes our recommendations for an optimised PIA methodology for the EU in terms of what a PIA should be, how it should be carried out, what it should contain and how organisations undertaking PIAs should be supported or encouraged. Several of these "best elements" are mentioned, albeit briefly, in Article 33 of the European Commission's proposed Data Protection Regulation. We refer to those. Where the best elements are absent, we recommend that decision-makers in the European Commission, Member States and industry take those into account in formulating an optimal PIA policy.

What a PIA should be

A PIA should go beyond a simple check that a project complies with legislation and engage stakeholders in identifying risks and privacy impacts that may not be caught by the compliance check. Article 33(4) says a data controller 'shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations' (European Commission, 2012).

Many PIA guidance documents, such as the ICO *Handbook*, emphasize PIA as a process, not simply an exercise aimed at producing a 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. Article 33, as currently drafted, seems to place its emphasis on preparation of the PIA report. If Article 33 is revised before the proposed Regulation is adopted, then the EC could add some wording that emphasises PIA as a process.

How and under what circumstances it should be carried out

PIAs should be undertaken with regard to any project, product, service, programme or other initiative, including legislation and policy. Article 33 says a PIA (or rather a data protection impact assessment) should be carried 'Where processing operations present specific risks to the rights and freedoms of data subjects' (European Commission, 2012). (The Article 29 Data Protection Working Party has suggested amending this provision by inserting the words "likely to" before "present" (Art. 29 WP, 2012: 16)

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.

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. Article 33 implies that a PIA should be conducted early when it refers to "the envisaged processing operations" (European Commission, 2012).

Several of the PIA guidance methodologies (e.g., Australia, UK) say that "Consultation with stakeholders is basic to the PIA process." 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 of gathering 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. As noted above, Article 33 contains a provision whereby data controllers shall seek the views of data subjects or their representatives.

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 of the relevant countries. Recital 72 of the proposed Data Protection Regulation, while it does not include cross-jurisdictional projects per se, does say 'There are circumstances under which it may be sensible and economic that the subject of a data protection impact assessment should be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity' (European Commission, 2012).

What it should contain

The PIA should identify information flows, i.e., who collects information, what information they collect, why they collect it, how the information is processed and by whom and where, how the information is stored and secured, who has access to it, with whom is the information shared, under what conditions and safeguards, etc. 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. Article 33 focuses on "data protection" only. Hence, this is a major limitation of the proposed Regulation as currently framed.

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. Article 33(2) contains a list of risks. The PIA should also include a discussion of what solutions to the privacy risks were identified, what potential changes were considered to mitigate those risks and how the system or technology was modified or changed to address those risks. The PIA should specify who undertook the PIA, how they can be contacted for more information and where to find further information and other sources of help and advice. Article 33 does not go into this detail.

How organisations should be supported or encouraged to undertake PIAs

PIA guidance documents should be aimed at not only government agencies but also companies or any organisation initiating or changing a project, product, service, programme, policy or other initiative that could have impacts on privacy. Article 33 refers to data controllers and does not limit itself to just government agencies. Hence, companies would also have to adhere to its provisions.

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. Article 33 does not go into this level of detail.

Although some PIA guidance documents, such as the New Zealand *Handbook* and the ICO *Handbook*, say that "no one size fits all" in PIA, 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. Article 33 specifies what a PIA report should contain "at least".

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. 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. 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 guidance more practical and effective. The New Zealand handbook has a useful bibliography of national and international PIA resources. Article 33 does not go into this level of detail.

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. Article 33 does not contain such a provision. 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 can balance the security and transparency interests. Article 33 makes no explicit mention regarding publication of the PIA report.

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. For example, in New Zealand, PIA is regarded as an "early warning system". Other PIA guidance documents have picked up on the same wording.

Article 33 refers only to the risks. There is no mention of the benefits. Privacy commissioners or other leaders should identify and publish particular PIA reports as examples of good practice. Article 33 does not contain any such provision. A PIA guidance document should be updated from time to time, as happens in several countries. Article 33 is silent on this. 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. Article 33 does not contain such a provision. PIA should be part of an organisation's overall risk management practice.

Privacy commissioners do not generally approve PIAs; however, they may review them and provide guidance on improving them. Article 33 does not contain such a provision. 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. Article 33(7) says 'The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment'.

CONCLUSION

Europe has an opportunity to develop a state-of-the-art PIA policy and methodology. It should benefit from the experience of others, notably the countries analysed in this paper, and construct a PIA framework based on the "best" elements of existing policies and methodologies, i.e., those elements recommended by the authors as well as other PIA experts. This paper has provided a comparative analysis of PIA methodologies in the six countries with the most experience of PIA and identified some of the elements that could be used in a European PIA policy and methodology. The findings of this paper can be used by policy-makers and industry decision-makers to "flesh out" the rather sketchy provisions for PIA in Article 33 of the proposed Data Protection Regulation. In the preceding section of this paper, we have identified which of our findings correlate with Article 33 and where there are lacunae in Article 33 that could be filled by our recommendations.

* * *

ACKNOWLEDGEMENTS

The paper draws on research performed for the European Commission's Directorate-General Justice under Grant Agreement number: JUST/2010/FRAC/AG/1137 – 30-CE-0377117/00-70. For more information and for a more extensive examination of PIAs, see the PIAF project website (www.piafproject.eu) and, in particular, the first PIAF deliverable.

[1] www.piafproject.eu. Last accessed: 17 March 2013.

[2] Wright (2011a) has identified seven types of privacy – the four identified by Clarke, plus privacy of location, privacy of thought and feeling, and privacy of the group or association.

[3] The UK Information Commissioner's Office *PIA Handbook* uses a similar definition (ICO, 2007).

[4] 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.

[5] 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.

[6] http://www.csa.ca/cm/ca/en/privacy-code. Last accessed: 17 March 2010.

[7] For contents of IMPIAs, see OPC, 2008.

[8]http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/PRIVACY_IMPACT_ASSESSMENT_OVERVIEW.ashx. Last accessed: 17 March 2013.

[9] See, for example: Department of Communities and Local Government, *Making Better Use of Energy Performance Data: Impact Assessment*, Consultation, March 2010; Department for Transport, *Impact Assessment on the Use of Security Scanners at UK Airports*, Consultation, March 2010.

[10] See http://www.whitehouse.gov/omb/memoranda/m03-22.html for a list of these examples.

REFERENCES

American Chamber of Commerce to the European Union (2012). 'AmCham EU position on the General Data Protection Regulation', Brussels, 11 July.

Article 29 Data Protection Working Party (2011). Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Brussels, Adopted on 11 February 2011. Available at:

http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf. Last accessed: 17 March 2013.

Article 29 Data Protection Working Party (2012). Opinion 01/2012 on the data protection reform proposals, Brussels, 23 March. Available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf. Last accessed: 17 March 2013.

Bamberger, K. A., and Mulligan, D. K. (2008). 'Privacy Decision making in Administrative Agencies', *University of Chicago Law Review*, 75 (1), pp. 75-107.

Bamberger, K. A., and Mulligan, D. K. (2012). 'PIA requirements and privacy decision-making in US government agencies' in D. Wright and P. De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer, pp. 225-250.

Bayley, R., and Bennett, C. J. (2012), 'Privacy impact assessments in Canada', in D. Wright and P. De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer, pp. 161-185.

Bennett, C. J. (2007). '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, October.

Bennett, C. and Raab, C. (2006). *The Governance of Privacy*, Cambridge, MA: MIT Press.

Cabinet Office (2008a). 'Data Handling Procedures in Government: Final Report', June. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf. Last accessed: 17 March 2013.

Cabinet Office (2008b). 'Cross Government Actions: Mandatory Minimum Measures', Section I, 4.4. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf. Last accessed: 17 March 2013.

Clarke, R. (1997, rev. 2006). 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', Xamax Consultancy. Available at:

http://www.rogerclarke.com/DV/Intro.html. Last accessed: 17 March 2013.

Clarke, R. (2009). 'Privacy Impact Assessment: Its Origins and Development', *Computer Law & Security Review*, 25 (2), pp. 123–135.

Clarke, R. (2011). 'An Evaluation of Privacy Impact Assessment Guidance Documents', *International Data Privacy Law*, 1 (2), pp. 111-120.

Clarke, R. (2012). 'PIAs in Australia: A work-in-progress report', in D. Wright and P. De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer.

De Hert, P. (2012). 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments', in D. Wright and P. De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer. Available at: http://www.springer.com/law/international/book/978-94-007-2542-3. Last accessed: 17 March 2013.

Dempsey, J. X. (2004). 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.

Department of Communities and Local Government (2010). *Making Better Use of Energy Performance Data: Impact Assessment*, Consultation, March. Available at:

http://www.legislation.gov.uk/ukia/2010/304. Last accessed: 17 March 2013.

Department of Homeland Security (DHS) (2007). *Privacy Technology Implementation Guide*, Washington, DC, 16 August.

Department of Homeland Security (DHS) (2010). *Privacy Impact Assessment Template*, Washington, DC.

Department for Transport (2010). *Impact Assessment on the Use of Security Scanners at UK Airports*, Consultation, March. Available at: http://webarchive.nationalarchives.gov.uk/20110130233603/http://www.dft.gov.uk/consultations/closed/2010-23/ia.pdf. Last accessed: 17 March 2013.

Edwards, J. (2012). 'Privacy Impact Assessment in New Zealand – A Practitioners' Perspective', in D. Wright and P. De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer, pp 187-204.

European Commission (2009). 'Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification', C (2009) 3200 final, Brussels, 12 May. Available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009H0387:EN:HTML. Last accessed: 17 March 2013.

European Commission (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January. Available at: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm. Last accessed: 17 March 2013.

Health Information and Quality Authority (HIQA) (2010a). *International Review of Privacy Impact Assessments*. Available at: http://www.hiqa.ie/resource-centre/professionals. Last accessed: 17 March 2013.

Health Information and Quality Authority (HIQA) (2010b). *Guidance on Privacy*

Impact Assessment in Health and Social Care, Dublin, December. Available at: http://www.hiqa.ie/resource-centre/professionals. Last accessed 17 March 2013.

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

Information Commissioner's Office (ICO, 2007b, 2009). *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 1.0, December 2009. Version 2.0, June 2009. Available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html. Last accessed: 17 March 2013.

Ministry of Justice (2010). Undertaking Privacy Impact Assessments: The Data Protection Act 1998, Ministry of Justice, 13 August. Available at: http://www.justice.gov.uk/downloads/information-access-rights/data-protection-act/pia-guidance-08-10.pdf. Last accessed: 17 March 2013.

New Zealand Government, Immigration Act (2009). Public Act 2009 No 51. Available at: http://www.legislation.govt.nz/act/public/2009/0051/latest/DLM1440303.html. Last accessed: 17 March 2013.

Office of Management and Budget (OMB) (2003). OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Washington, DC, 26 September. Available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html. Last accessed: 17 March 2013.

Office of the Information and Privacy Commissioner of Alberta (OIPC) (2009). Privacy Impact Assessment (PIA) Requirements For use with the Health Information Act, January. Available at: http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf. Last accessed: 17 March 2013.

Office of the Privacy Commissioner (2006, 2010). *Privacy Impact Assessment Guide*, Sydney, NSW. Available at: http://www.privacy.gov.au. Last accessed 17 March 2013. The *PIA Guide* can also be downloaded from http://www.oaic.gov.au/publications/guidelines.html#privacy_guidelines. Last accessed: 17 March 2013.

Office of the Privacy Commissioner (New Zealand) (OPC) (2007). *Privacy Impact Assessment Handbook*, June.

Office of the Privacy Commissioner (OPC) (2008). Guidance Note for Departments Seeking Legislative Provision for Information Matching, Appendix B, New Zealand, 16 May. Available at: http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching/#appendix. Last accessed: 17 March 2013.

Office of the Privacy Commissioner (OPC) (2010). Operating programmes, New Zealand, 30 June. Available at: http://privacy.org.nz/operating-programmes/. Last accessed: 17 March 2013.

Privacy Commissioner of Canada (OPC) (2007). *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report, October. Available at: http://www.priv.gc.ca/information/pub/ar-vr/pia_200710_e.cfm. Last accessed: 17 March 2013.

Rotenberg, M. (2006). 'The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11', SSRN WPS, September, pp. 24-25.

Tancock, D., Pearson, S. and Charlesworth, A. (2010). '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 August, published 30 September, pp. 118-125. Available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5593260. Last accessed 17 March 2013.

Teufel III, H. (2008). *Privacy Policy and Guidance Memorandum*, Department of Homeland Security, Memorandum Number 2008-02, 30 December.

Treasury Board of Canada Secretariat (2002). 'Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks', Ottawa, 31 August. Available at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp. Last accessed: 17 March 2013.

Treasury Board of Canada Secretariat (2008). Policy on Privacy Protection, Ottawa, 1 April. Available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text. Last accessed: 17 March 2013.

Treasury Board of Canada Secretariat (2010). Directive on Privacy Impact Assessment, Ottawa, 1 April. Available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text. Last accessed: 17 March 2013.

US Government. E-government Act of 2002 (2002), Public Law 107-347.

Available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm. Last accessed: 17 March 2013.

Warren, A. and Charlesworth, A. (2012). 'Privacy Impact Assessment in the UK' in D. Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer, pp. 205-224.

Wright, D. (2011a). Appendix to PRESCIENT Deliverable D1, a report prepared for the European Commission, Brussels. Available at: http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf. Last accessed: 17 March 2013.

Wright, D. (2011b). 'Should Privacy Impact Assessments be Mandatory?' *Communications of the ACM,* 54 (8), pp. 121-131.

Wright, D., Wadhwa, K. De Hert, P. and Kloza, D. (eds) (2011). 'A Privacy Impact Assessment Framework (PIAF) Deliverable D1', A Report of the PIAF Consortium Prepared for the European Commission, September. Available at: www.piafproject.eu. Last accessed: 17 March2013.

Wright, D., and Wadhwa, K. (2012). 'A step-by-step guide to privacy impact assessment', Paper presented to the second PIAF workshop, Sopot, Poland, 24 April. Available at: www.piafproject.eu. Last accessed: 17 March 2013.