available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Report

PIAs and risk assessment

Privacy Impact Assessments: International experience as a basis for UK Guidance

Adam Warren[a], *Robin Bayley*[b], *Colin Bennett*[b], *Andrew Charlesworth*[c], *Roger Clarke*[d], *Charles Oppenheim*[e]

[a]*Department of Geography, Loughborough University, UK*
[b]*Linden Consulting, Inc., Victoria, BC, Canada*
[c]*School of Law, Bristol University, UK*
[d]*Xamax Consultancy Pty Ltd., Chapman, ACT, Australia*
[e]*Department of Information Science, Loughborough University, UK*

ABSTRACT

In July 2007, the UK Information Commissioner's Office commissioned a team of researchers, coordinated by Loughborough University, to conduct a study into Privacy Impact Assessments (PIAs). This was with a view to developing PIA guidance for the UK. The project resulted in two key deliverables: a study of the use of PIAs in other jurisdictions, identifying lessons to be learnt for the UK; and a handbook that can be used to guide organisations through the PIA process, taking into account the provisions of the UK Data Protection Act (DPA) 1998. This paper draws on the original research undertaken as part of that assignment to provide an overview of the ICO-funded project and the extent to which PIAs can be used in the current UK context. Firstly, the authors consider the findings of the comparative study and how the UK experience can be informed by developments overseas. Secondly, the paper outlines the development of the handbook during the course of the project and the extent to which it has been influenced by the overseas experience and the current UK political context. Thirdly, aspects of the handbook itself are considered and explained. Particular attention is paid to: its format; its key features; and feedback received on an interim version from a focus group of experienced data protection and project management practitioners. Finally, the paper concludes by stating why the study and the handbook provide appropriate tools for guidance in the current UK context, and how they can be developed further.

1. Introduction

Privacy Impact Assessments (PIAs) first came into general usage in North America and Australia in the late 1990s. They represented a development of existing data protection, or information privacy, statutes that had been enacted in many Western democracies from the early 1970s onwards. These statutes were based on a number of fair information principles, often enforced by an independent oversight body. However, over the last two decades, a number of factors necessitated the development of more specific policy instruments. These included: the move from the 'databank' to the

0267-3649/$ – see front matter © 2008 Adam Warren, Robin Bayley, Andrew Charlesworth, Colin Bennett, Roger Clarke, Charles Oppenheim. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2008.03.003

more decentralised networked information systems, providing a range of new data processing and manipulation techniques; the blurring of the distinction between public and private sectors as a result of outsourcing and privatisation; and the introduction of a variety of intrusive surveillance techniques (ICO, 2007a: 4–5). These factors have resulted in a proliferation of policy instruments for privacy, such as privacy seals, standards and codes of practice. Moreover, as public and private sector organisations have moved towards conducting risk assessments, there was general recognition within the community of data protection officials that more prospective tools were required to anticipate, and mitigate, privacy problems.

PIAs have been thus defined as a systematic risk assessment tool that can be usefully integrated into decision-making processes (Stewart, 1996a,b, 1999; New Zealand, 2002; Clarke, 2004; Bennett and Raab, 2006). Although the processes involved in conducting a PIA vary widely, they are now in use across much of the English-speaking world, in particular in Canada, Australia and the United States. They are often developed in conjunction with electronic government initiatives and have been most commonly used by public sector organisations. In the private sector, related techniques are typically known under other terms such as 'privacy strategy formulation' and 'privacy issues analysis'. Regardless of the terminology, the authors found that effective PIAs should do the following:

(i) Conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified.
(ii) Assess the impacts in terms broader than those of legal compliance.
(iii) Be process rather than output-oriented.
(iv) Be systematic.

Consequently, PIAs differ from privacy audits, the latter being defined as 'the detailed analysis of systems that are already in place against a prevailing legal, management or technology standard' (ICO, 2007a: 1). The key benefits of PIAs, therefore, can be summarised as

- The avoidance of loss of trust and reputation.
- The identification and management of risks.
- Cost avoidance.
- Meeting and exceeding legal requirements (ICO 2007b).[1]

The guidance materials from various overseas regulators have described these benefits in some detail. For example, the Privacy Commissioner of New Zealand has stated that PIAs provide an 'early warning system' for agencies (New Zealand, 2002: 6). In particular, they help

- 'to inform decision-makers';
- 'to assuage alarmist fears';
- 'to alert the complacent to potential pitfalls';
- 'to ensure that a business is the first to find out about privacy pitfalls in its project, rather than learning of them from critics or competitors';
- 'to save money and protect reputation';
- 'to bring privacy responsibility clearly back to the proponent of a proposal';
- 'to encourage cost-effective solutions since it is cheaper to do things at the design phase to meet privacy concerns than attempt to retrofit after a system is operational' (New Zealand, 2002: 13).

For a number of years, the UK Information Commissioner's Office (ICO) – responsible for the regulation of data protection legislation in the UK – has called for PIAs to be considered, especially in the design of large-scale government projects including the National Identity Register (House of Commons, 2004; ICO, 2004; ICO, 2005). However, their adoption in the UK has been extremely slow. A PIA feasibility study was conducted in relation to social care provision in Scotland (Raab et al., 2004), and a further PIA has been performed by the Northern Ireland Valuation and Lands Agency (Northern Ireland, 2006). However, recent scandals – such as the loss of personal data records for 25 million individuals and 7.25 million families receiving child benefits by Her Majesty's Revenue and Customs (HMRC) (BBC News, 2007) – have demonstrated a clear need for organisations to comprehensively assess risks posed to privacy by new or existing systems. This has also resulted in the Information Commissioner's Office being approached by a number of public and private sector organisations, 'almost on a confessional basis', to bring their attention to problems they had encountered with data security (House of Commons, 2008).

In July 2007, the ICO commissioned a team of experts from Canada, Australia and the UK,[2] led by Loughborough University, to conduct a project into PIAs with the aim of assisting their work in promoting the use of the tool in the UK. The project produced two key deliverables:

(i) A study into the use and effectiveness of PIAs in other jurisdictions, identifying lessons for the UK and highlighting features that should be incorporated into a UK PIA process.
(ii) A user-friendly handbook for use by practitioners, to guide them through the PIA process in line with relevant UK legislation.

This paper considers some of key findings of this project, stating why the study and handbook provide appropriate initial guidance in the current UK context, and how they can be developed further.

[1] Further details of the benefits of conducting a PIA are outlined in the handbook produced by the project team, under the subheading 'Why do a Privacy Impact Assessment': http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html.

[2] The research team comprised the authors of this paper, with Charles Oppenheim as Project Director.

2. The study: application and effects of PIAs overseas

The study reviewed PIA models in Canada (and relevant provinces), Australia (including all states and territories), United States, New Zealand and Hong Kong. The research in these jurisdictions involved three strands. Firstly, an analysis was undertaken of relevant legislation, policy and PIA tools. Secondly, interviews were conducted with key policy-makers in government and data protection regulators to determine the lessons learned and any perceived shortcomings arising from their PIA processes. Thirdly, a limited number of interviews were also conducted in organisations that had made use of PIAs to capture the practitioner perspective, in particular, the extent to which they drew on existing PIA models and liaised with national oversight bodies. In addition, significant, but less comprehensive research was undertaken with regard to the jurisdictions of the European Union. PIAs have to date gained little formal traction in the EU Member States, but a range of 'prior checking' mechanisms, based on Article 20 of the EU Data Protection Directive, are provided for in legislation, and sometimes actively used, in at least 16 Member States.[3]

The remainder of this section draws heavily on the main report into the study produced for the ICO (2007a). Responsibility for the research was split between the team members, who used a common interview protocol, adapted to suit local circumstances. The interviews were conducted either in person or by telephone from early July to the end of August 2007. All interviewees were asked if they could be cited on the record, although the jurisdiction reports most frequently cited the organisational affiliation of the individual interviewed. In addition to formal interviews, contact was made with other experts to confirm facts or request publications. This was complemented by documentary research in the various regions and in relevant literatures.

2.1. *Summary findings*

The general findings from the study are detailed in the Executive Summary of the report (ICO, 2007a, vi and vii). Extracts are provided below:

- PIAs are a good idea and are increasingly recognised as such by privacy commissioners, government agencies, private corporations and privacy advocates. They help to address the increasing concerns about privacy within advanced industrial societies;
- PIAs have been spreading around the advanced industrial world as a result of: legislative requirements; policy guidance by central government agencies; recommendations by privacy and data protection commissioners;
- Organisations have recognised that PIAs can expose and mitigate privacy risks, avoid adverse publicity, save money, develop an organisational culture sensitive to privacy, build trust and assist with legal compliance;
- To be valuable, PIAs need to offer a prospective identification of privacy risks *before* systems and programmes are put in place;
- Many exercises that are called PIAs are little more than legal compliance checks. To be meaningful, PIAs have to consider privacy risks in a wider framework that takes into account the broader set of community values and expectations about privacy;
- PIAs are more than the end-product or statement. They refer to an entire process of assessment of privacy risks. PIA reports do not necessarily reveal the changes made to the initiative during the PIA process;
- PIAs are only valuable if they have, and are perceived to have, the potential to alter proposed initiatives in order to mitigate privacy risks. Where they are conducted in a mechanical fashion for the purposes of satisfying a legislative or bureaucratic requirement, they are often regarded as exercises in legitimation rather than risk assessment;
- PIA processes vary across a number of dimensions: the levels of prescription, the application, the circumstances that might trigger PIAs, the breadth of the PIA exercise, the agents who conduct PIAs, the timing, the process or review and approval and the level of public accountability and transparency;
- The scope and depth of the PIA needs to be sensitive to a number of crucial variables: the size of the organisation; the sensitivity of the personal data; the forms of risk; the intrusiveness of the technology. A PIA screening process is commonly used to determine whether a PIA is required, and if so, the form it should take.

PIAs appeared to be more effective where:

> *…they are part of a system of incentives, sanctions and review, and/or where they are embedded in project workflows or quality assurance processes (ICO, 2007a, v).*

An important example of a relevant business process is threat risk assessment. This is commonly used in business, and in the public sector in some jurisdictions, to determine threats to information and IT assets. In Ontario, for example, the PIA process is very much seen as linked to the threat/risk assessment process in the development and supply of government services (ICO, 2007a, Appendix C, 22). Likewise, in the UK, there is potential for PIAs to be integrated into the existing Office of Government Commerce Gateway (OGC)

[3] European Communities (1995). *Directive 95/46/EC*, 1995 O.J. L 281/31. The Directive requires that DP supervisory authorities should have effective powers of intervention, including that of delivering opinions before processing operations are carried out. In order to enable this power of pre-processing intervention, Article 20 requires that processing operations likely to present specific risks to the rights and freedoms of data subjects should be examined prior to their start. National implementations vary widely. In the UK, s. 22 Data Protection Act 1998 provides for a version of 'prior checking' for those types of processing specified in an Order made by the Secretary of State. No Orders have been made.

Review Process for Programmes and Projects.[4] However, organisations should guard against producing PIA documentation in order to satisfy another stage in the project cycle.[5] A PIA should always set out to be an open-ended, comprehensive and serious analysis of proposed systems and projects.

The effectiveness of PIAs is also enhanced when individuals responsible for completing PIAs have a good project knowledge and access to various expertise including 'privacy law and practice, information security [and] records management' (ICO 2007a, v). Processes of external review and use of external consultants for larger projects are recommended, as is transparency, which 'enhances trust in the initiative being proposed' (ICO 2007a, vii and viii).

2.2. *Recommendations for a UK PIA*

The project team were sensitive to the fact that there is currently no formal Parliamentary backing for PIAs and that the ICO can only recommend their completion. Therefore the PIA process had to be perceived to be of benefit to data controllers. The ICO – in commissioning the study and the development of the handbook – signalled its intent to advocate for the tool.

Establishing a framework for PIA processes is not an overnight matter. It has taken some of the jurisdictions 5–10 years to reach their current position, and many regulators see scope for improvement. In this respect, the ICO has the clear advantage as it is able to learn from experiences elsewhere, especially from jurisdictions such as Australia and Ontario which have attempted to encourage PIAs through powers of moral suasion. The project team recommended a structured and timetabled roll-out of PIAs, with attention being given to developing expertise in the conduct of PIAs (ICO, 2007a: 31). In December 2007, the ICO signalled its intention to 'soft launch' the handbook, and to provide a mechanism for practitioner feedback over a 12 month period.[6]

With these lessons in mind, and having taken consideration of the UK context, the handbook for UK practitioners has been designed on the basis that the following features are incorporated into the UK PIA process. The process should

- be a comprehensive risk assessment exercise, using privacy concepts beyond those entailed in detailed data protection legislation;
- be more process-oriented than output-oriented;
- be integrated, where possible, into existing business and management processes, rather than seen as an 'add-on';
- employ a screening tool to determine the scale of the PIA to be conducted;
- provide flexibility of scale. The guidance should indicate the circumstances when full PIAs may be necessary, where smaller-scale PIAs may be appropriate or where PIAs are unnecessary;
- be conducted at a stage of the project when the direction of the initiative may be influenced;
- be transparent and accountable. The process should include external consultation where appropriate, and reports should be published or otherwise made available;
- define organisational responsibilities. The individual responsible for compliance with data protection within the organisation should review the PIA. A senior executive should approve the PIA;
- consider whether external review and approval are appropriate. This should involve interaction between the regulator and the organisation (ICO, 2007a: 34–36).

These recommendations were informed, in part, by guidance on PIAs overseas, including hard copy handbooks, such as those produced by the Australian Privacy Commissioner (2006), the New Zealand Privacy Commissioner (2002) and the Ontario Management Board Secretariat (2001).[7] Moreover, the team noted with interest the web-based e-learning tool, published by the Canadian government's Treasury Board Secretariat (TBS) in 2003.[8] This can provide a useful training tool, allowing project personnel to become cognisant with PIA terminology and definitions. The TBS version has required minimal updating, and the team are confident that a similar product could be developed for the UK.

3. The handbook – development and screening tool

3.1. *Development*

Given the UK political context, discussed above, the project team aimed to produce a PIA process that is straightforward whilst requiring organisations to achieve some depth. There had been some previous UK work in this area. For example, the Northern Ireland Valuation and Lands Agency undertook

[4] OGC Gateway Reviews deliver a 'peer review' in which independent practitioners from outside the programme/project use their experience and expertise to examine the progress, and likelihood of successful delivery, of the programme or project. They are used to provide a valuable additional perspective on the issues facing the internal team, and an external challenge to the robustness of plans and processes. Refer: http://www.ogc.gov.uk/what_is_ogc_gateway_review.asp.

[5] In the United States, for example, the *Electronic Government Act* of 2002 requires that federal agencies undertake PIAs 'before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information.' However, as there is no requirement under the E-Government legislation for outside consultation, the project team's research indicated that procedures seem to have developed to emphasise the importance of PIAs as 'pre-decisional' instruments for the benefit of internal review and analysis. In this context, whilst it may be better to have PIAs conducted and published than not, this circumstance does present a series of questions about whether the internal procedures really do result in significant changes to a programme in response to internal arguments about privacy risks.

[6] The ICO have stated that they are keen for organisations to 'test' the handbook over a period of 12 months from its launch. Information on how to submit feedback is due to be released shortly. Refer: http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_conference.aspx.

[7] This guidance was under review when the team conducted its research (July–October 2007).

[8] Refer: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a_e.asp.

a PIA in 2006 and, in the mobile telecommunications sector, Vodafone have sought to incorporate wide-ranging privacy risk assessments into the early stages of project development. UK organisations were, therefore, already beginning to integrate a form of privacy risk assessment into their existing business processes. In other jurisdictions, PIAs had been incorporated into:

- IT procurement policy, ensuring that privacy issues and concerns are fully identified, documented and addressed as part of the approval process;
- Threat Risk Assessment process;
- General reputation management.

When working on the handbook, the team aimed to devise guidance that required organisations to commit only the level of resources commensurate with the risks involved. It was therefore decided at an early stage that specifying a single, catch-all, PIA would not be appropriate. This was, firstly, because the degree of risk created by projects varies enormously. Secondly, projects vary widely – from updating of small databases to implementing legislative proposals such as ContactPoint, created under the Children Act 2004 (s. 12).

The team, therefore, decided to

(i) recommend the use of a PIA screening tool, ensuring that organisations are diverted into one or more streams – Full-Scale PIA, Small-Scale PIA, Privacy Law Compliance Check, Data Protection Compliance Check – according to the characteristics of the project they are undertaking;
(ii) present the PIA 'Handbook' as a tiered website, so that each organisation only needs to view the sections that are relevant to it.

3.2. *Screening tool*

The screening tool allows practitioners to conduct a limited preliminary evaluation, establishing the extent to which their organisation needs to invest in the PIA process. An outline is presented in Fig. 1.

The screening tool comprises four steps, beginning with the 'hard', strategic questions, and then moving down the scale in terms of complexity and cost. This approach was decided on for a number of reasons. Firstly, if a PIA is necessary, then it needs to be performed early, well before the compliance checks, as it is likely to result in changes to the project design. Secondly, putting the steps in this sequence allows the project manager more notice and more time to factor the PIA into the project schedule. Moreover, it is consistent with privacy being seen as a matter of strategic significance rather than just an administrative add-on.

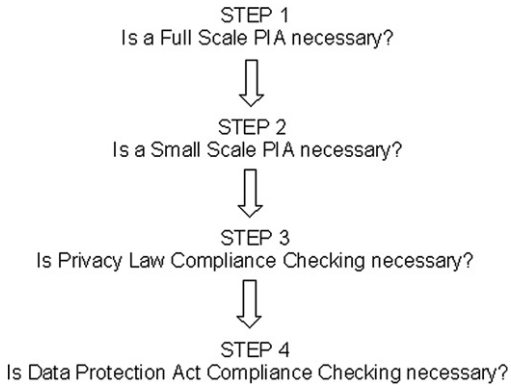

Fig. 1 – PIA screening tool – outline.

3.2.1. *Step 1 – is a Full-Scale PIA necessary?*

The Full-Scale PIA refers to the comprehensive PIA process. In the handbook, the need for this is evaluated via 11 questions, covering a number of privacy risk factors under sub-headings such as 'Technology', 'Identity' and 'Multiple Organisations'.

The questions include:

- *Does the project apply new or additional information technologies that entail substantial potential for privacy invasiveness?*
- *Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?*
- *Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?*

If it is decided that the project does not warrant a Full-Scale PIA – if the 11 questions are answered 'no' or 'n/a' – there may still be privacy impacts that are potentially serious, or not well understood. These are addressed under Step 2.

3.2.2. *Step 2 – is a Small-Scale PIA necessary?*

The Small-Scale PIA is designed for projects that do not warrant as great an investment of time and resources as Full-Scale PIAs, but still require attention. In the handbook, the need for this version of the PIA is evaluated via 15 tests – under similar headings to those used for Step 1. The change in emphasis can be seen by comparing the three questions used to illustrate the Step 1 evaluation above, with the three questions listed below:

- *Does the project involve new or inherently privacy-invasive technologies?*
- *Does the project involve additional use of an existing identifier?*
- *Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?*

If only one or two aspects give rise to privacy concerns, then the PIA process should focus on them. If, however, multiple questions are answered in the affirmative, then a Full-Scale assessment may be more appropriate. In either case, it is necessary to continue with Steps 3 and 4 to determine whether compliance checking should also be included in the project schedule.

3.2.3. *Steps 3 and 4 – are privacy law and/or data protection compliance checks necessary?*

Compliance checking involves a series of tests to ensure the project complies with relevant laws. It is advised that compliance checks are conducted at the end of the project as an

entirely separate activity to the PIA itself. In the handbook, compliance checking involves two, closely related, activities:

(i) An initial set of tests to check whether laws other than the UK DPA 1998, and that may also have privacy implications, are relevant. They include: law of confidence; Human Rights Act 1998; Regulation of Investigatory Powers Act 2000; and the Privacy and Electronic Communications Regulations 2003.
(ii) A second, relatively straightforward set of tests to establish whether the provisions of the DPA 1998 are applicable.

4. The handbook – PIAs and compliance checking

This section will consider in turn the processes involved in the four pathways presented to practitioners to assess privacy impacts posed by the introduction of new projects and systems, or the revision of existing schemes.

4.1. *Full-Scale PIAs*

Full-Scale PIAs should be conducted on projects that have considerable implications for privacy. Examples include: the application of new or additional information technologies that entail substantial potential for privacy invasiveness, such as smart cards, RFID tags and logging of electronic traffic; government agencies providing joined-up government initiatives, which could facilitate the breakdown of personal data silos[9]; and new or significantly changed handling of personal data that is of particular concern to people, including data categorised as 'sensitive' under section two of the DPA 1998.[10]

The Full-Scale PIA comprises five phases, outlined in Fig. 2.

The following commentary summarises each phase. Further detail is available in the published handbook (ICO, 2007b).

4.1.1. *Phase 1: preliminary phase*

The purpose of Phase 1 is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently. The suggested deliverables are a project plan and a project background paper. The project plan deals with the phases, tasks and deliverables of the project, whilst the project background paper establishes the basis for discussions with stakeholders. The latter should contain a clear and well-argued case for the project as a whole, and particularly for those features that have the greatest potential for negative privacy impacts. Considerations include:

- a description of the context or setting in which the proposal is being brought forward, including relevant social, economic and technological considerations;
- a statement of the motivations, drivers or opportunities underlying the project;
- a statement of the project's objectives, scope and business rationale;
- a description of project's design;
- an initial assessment of potential privacy issues and risks;
- the business case;
- lists of involved organisations, stakeholder groups[11] and advocates (ICO, 2007b).

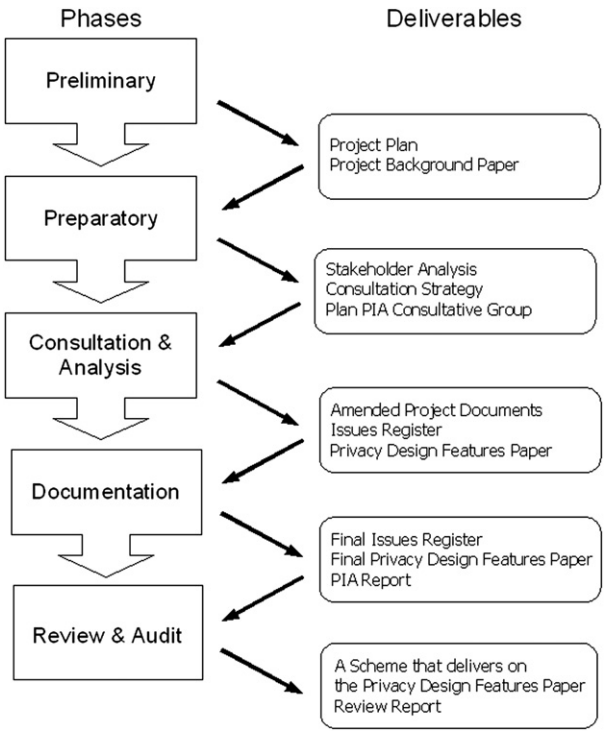

Fig. 2 – Full-Scale PIA – phases and deliverables.

4.1.2. *Phase 2: preparatory phase*

The purpose of this phase is to make the arrangements needed to enable Phase 3, the critical phase, to run smoothly. The suggested deliverables are a stakeholder analysis, ensuring that major players in the project have been identified, and a consultation strategy, ensuring that discussions with

[9] A 'data silo' is a database or set of files that is used by a particular application and is not integrated with other databases or sets of files.

[10] Sensitive personal data include personal data relating to the data subject's: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; sexual life; commission or alleged commission of any offence; proceedings or any committed or alleged offence.

[11] Individuals or groups that perceive themselves to have a significant interest or 'stake' in the project, and that accordingly expect to have involvement in the project process. They include the organisation itself, other participating organisations and the affected public.

Table 1 – Key features of issues register and privacy design features paper

Document	Purpose	Format	Advantages
Issues register	Records the privacy issues that have been identified, and states how the organisation intends to avoid or ameliorate them.	In large projects, to be a separate document, maintained over time. In other cases it could take the form of a progressively changing attachment to meeting minutes, or a webpage.	More convenient when conducting the PIA.
Privacy design features paper	A list of the characteristics of a scheme that have been devised in order to address key privacy issues. This paper will usually only be necessary for the larger projects.	A separate document, probably prepared late in the consultation and analysis phase.	More convenient when reviewing/auditing the PIA process.

stakeholders are effective. Key considerations of the consultation analysis include:

- a sufficient diversity of participants to ensure that all relevant perspectives are represented;
- multiple rounds of:
  - information provision by the organisation;
  - events that enable interactions among the various stakeholders;
- assimilation of the information provided by all parties into the subsequent rounds of design and implementation activities.

As part of the consultation strategy, it is suggested that organisations establish a PIA consultative group, comprising relevant stakeholder groups such as individuals from the organisation itself, from participating organisations and from the affected public.

4.1.3. *Phase 3: consultation and analysis phase*

This phase is critical to the project's success. Its purpose is to ensure that problems are identified early, effective solutions are found promptly, and that the project design is adapted to embody those solutions.

The suggested deliverables for this phase are changes to the relevant project documents, an issues register and/or a privacy design features paper. The nature of these documents is summarised in Table 1. This phase generally involves repeating the exercise a number of times throughout the project lifecycle. The most effective approach is to conduct the exercise first at the stage of project initiation, and then to arrange subsequent run-throughs to correspond with the later phases of the project (i.e. requirements analysis; logical design; system design; and construction, implementation and operation of the new system).

4.1.4. *Phase 4: documentation phase*

The purpose of this phase is to document the PIA process and its outcomes. The suggested deliverable is a PIA report. However, it is important to reiterate that the main benefits to the organisation arise from the PIA process itself – in the form of learning and adaption to circumstances – rather than from publishing a document. Nevertheless, the PIA report does have some advantages. It provides, for example:

- an element of accountability, demonstrating that the PIA process was performed, and was performed appropriately;
- a basis for post-implementation review;
- a basis for audit (from outside the project);
- corporate memory, ensuring that the experience gained during the project is available to those conducting further iterations of the PIA if original staff have left the organisation.

4.1.5. *Phase 5: review and audit phase*

The purpose of this phase is to ensure that the tasks arising from the Phase 4 are carried through into the implemented project. The suggested deliverables are completion of the undertakings given in the privacy design features paper (if applicable, or in documents such as minutes and media releases) and preparation of a review report. Organisations could integrate this phase into an appropriate stage in the lifecycle of the overall project or build it into the organisation's internal or external audit processes.

4.2. *Small-Scale PIAs*

Small-Scale PIAs are designed to assess projects whose privacy implications are specific rather than substantial or extensive. Examples include: the introduction of security cards for staff to control entry to buildings; the addition of a further data item to an existing database; and the application of a new technology to an existing purpose, for instance, replacing barcode technology with a contact-based chip containing the same data. Depending on circumstances, some of these applications do have the potential to become Full-Scale PIAs, for example, if the personal data are highly sensitive or the technology untested.

The process for Small-Scale PIAs can be delegated to less senior staff, although executive oversight is still required. It can use the same phase structure as Full-Scale PIA, but is much briefer, for example, organisations may not need to establish a PIA consultative group. Where the organisation has an established privacy strategy and experience in the processes involved, a Small-Scale PIA may be able to be completed in a few hours.

4.3. *Privacy law compliance check*

In the handbook, the need for a compliance check is linked to three key questions. If any of the three are answered 'Yes',

then it is suggested a privacy law compliance check is conducted:

> 1. Does the project involve any activities (including any data handling) that are subject to privacy or related provisions of any statute or secondary legislation, other than the Data Protection Act?

Examples include:

- Human Rights Act 1998, in particular Schedule 1, Article 8 (Right to Respect for Private and Family Life) and Article 14 (Prohibition of Discrimination).
- Regulation of Investigatory Powers Act 2000 and Lawful Business Practice Regulations 2000.
- Privacy and Electronic Communications Regulations 2003.
- Data Retention (EC Directive) Regulations 2007.
- Sectoral legislation, for example, Financial Services and Markets Act 2000.
- Statutory codes, for example, the Information Commissioner's CCTV Code of Practice (2000).[12]

Where projects are cross-jurisdictional, they may include the laws of other countries. For example, organisations dealing with the United States may need to be aware of the provisions of the Gramm–Leach–Bliley Financial Modernization Act 1999, the Health Insurance Portability and Accountability Act 1996, the Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act 2003, the Sarbanes–Oxley Act 2002, as well as state laws such as California's Security Breach Information Act.

> 2. Does the project involve any activities (including any data handling) that are subject to common law constraints relevant to privacy?

In particular, it is suggested that users consider confidential data relating to a person and the emerging tort of privacy.

> 3. Does the project involve any activities (including any data handling) that are subject to less formal requirements relevant to privacy?

In particular, practitioners should consider industry standards, such as the ISO/IEC 27002:2005 Information Security Standard,[13] and industry codes, for example, the NHS Code of Practice on Confidentiality (Department of Health, 2003).

In terms of specific guidance to assist compliance checking, the project team have produced a template for the direct marketing aspects of the Privacy and Electronic Communications Regulations (PECR) 2003 (ICO, 2007a).

4.4. *Data protection compliance check*

The organisation has a legal obligation to ensure that the project process, the resulting design and the personal handled are compliant with the DPA 1998. The need for a data protection compliance checklist is linked to two questions.

> 1. Does the project involve the handling of any data that is personal data, as that term is used in the Data Protection Act?

> 2. Even if the organisation claims that the project is covered by one of the limited forms of exemption and exception available under the Act, does the organisation have a policy position of taking the Data Protection Principles into account?

A template is provided to assist practitioners in checking project compliance against the Data Protection Principles (ICO, 2007b).

5. Focus group feedback

The ICO were keen to ensure that practitioners had a stake in the development of the handbook. 'Road-testing', in the sense of conducting a PIA using the handbook developed by the project team, was clearly unrealistic in the 16-week project timeframe. Instead, it was agreed that a focus group comprising data protection practitioners would be convened to consider an early draft of the handbook.

The focus group met in September 2007.[14] It comprised 12 representatives from central government, local government and the private sector – all with considerable experience of data protection and project development at senior level. For ease of reference and due to the compressed time parameters of the project, participants were sent both a hard copy of the handbook in PDF format – running to 90 pages – and a link to the electronic version. Approximately one-third of the group were or had been engaged in some form of 'PIA process', even if it was not referred to as such. Those already carrying out assessments did so not because they were compelled to do so, but because they found the process valuable in terms of management decision-making and as part of threat risk assessment process. One of the clear messages that came of the session was that there was support for guidance in methods of

[12] The Code of Practice is currently under revision (ICO, 2007c).

[13] Refer: http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/.

[14] The focus group met approximately two thirds of the way through the project.

incorporating PIAs into existing business or management processes.[15]

However, the group did express some concerns – a number of which had been anticipated by the team – and made some recommendations for further development. Firstly, the handbook as it stood (the focus group saw the third full draft) was perceived to be too resource intensive for many organisations. This can be in part explained by the focus group members making greater reference to the hard copy, than the electronic version that the ICO intended organisations to use. In reality, the pathway approach meant that a practitioner would not need to see all the material.[16] Secondly, it was suggested that the draft handbook was simply trying to achieve too much, in terms of the size, scope and nature of the audience it was aimed at. In fact, the screening tool was specifically created to guide the user down one of a number of pathways – Full-Scale PIA, Small-Scale PIA, compliance check. The final handbook is deliberately flexible: it is advisory, not mandatory; it enables users to devise a PIA process to fit their specific needs; and it provides guidance on many aspects that may or may not be relevant in particular circumstances.

Finally, the focus group participants made some suggestions for improvement. They included:

(i) Use cases that outlined the benefits of PIA processes and demonstrated where they might best fit within an organisation's business processes.
(ii) Tools that were customisable to different business environments or designed for specific business environments, for example, use of tailor-made Q&As and FAQs.
(iii) Tools that would help practitioners focus and clarify questions about projects, services and other developments to the ICO, that tell the story of the project to the ICO in a manner that would facilitate effective feedback.
(iv) A request for the ICO to work to harmonise its PIA guidance with, or embed it within, contemporary project management processes such as the OGC's Gateway process.

The first suggestion has subsequently been addressed with use cases being incorporated into the final version of the handbook. The second suggestion, regarding customisable tools, went beyond the scope of the project, which was to produce a handbook. However, the team have provided a series of questions as part of the screening process and two structured templates for the aforementioned compliance checks. The third point has been addressed in the section of the handbook entitled 'Preparing for the PIA Screening Process', where the team recommend organisations to follow three steps: (a) preparing a project outline; (b) undertaking a stakeholder analysis; (c) performing an environmental scan, researching information about prior projects of a similar nature. Finally, the project team were in agreement with the fourth suggestion made by practitioners. Even though it, again, went beyond the scope of our project, the team have tried to ensure that there is nothing in the handbook to impede the possible harmonisation of PIA guidance with, or embedding of it within, existing project management processes.

In summary, the focus group was a valuable exercise. In many ways, it confirmed the direction the team were taking and assisted the development of certain elements of handbook, as well as giving other elements – such as the stated benefits of PIAs – greater prominence. In terms of further suggestions for improvement, the authors recommended that the ICO consider issuing bespoke guidance for specific categories of small projects and assist in the development of an e-learning tool that, as mentioned above, has been used to good effect in Canada to educate federal employees about privacy and the fundamentals of PIAs. Products could be tailored towards the UK public and private sectors, and easily accessible courses could be provided in the management, coordination and review of PIAs.

6. Conclusions

This research is the first officially sanctioned work on Privacy Impact Assessments in the UK. In that respect, the study and the handbook represent groundbreaking work, which has already attracted interest from government departments. It is also timely, given the highly publicised losses of personal data by central government departments and the private sector. We have produced what is intended to be a flexible, dynamic tool, informed by the findings of an original piece of research into PIAs across the globe. The size and scope of projects vary, and the handbook takes this into account with its use of multiple pathways enabling organisations to follow a PIA process that fits their specific needs. Yet this is just the first stage. Its further development will be informed by the evolving UK legal and political context, and at least equally pertinently, by practitioner feedback.

Adam Warren (*A.P.Warren@lboro.ac.uk*), *Department of Geography, Loughborough University;* **Robin Bayley & Colin Bennett**, *Linden Consulting, Inc., Victoria, BC, Canada;* **Andrew Charlesworth**, *School of Law, Bristol University,* **Roger Clarke**, *Xamax Consultancy Pty Ltd., Chapman, ACT, Australia, and* **Charles Oppenheim**, *Department of Information Science, Loughborough University*.

Acknowledgements

We wish to thank the Information Commissioner's Office for funding this research and for permission to publish information arising from the project deliverables. We also wish to thank Professor Saxby for his interest in this paper and the anonymous referee(s) for providing feedback.

[15] The OGC Gateway Review for Programmes and Projects was cited as an example.

[16] Indeed, when pressed for a 'realistic' size for a PIA handbook, or template, even the 40–50 page hard copy versions that can be found in jurisdictions such as Ontario and New Zealand were regarded as too long.

REFERENCES

Australia Office of the Federal Privacy Commissioner. Privacy impact assessment guide. Sydney, Australia: Office of the Privacy Commissioner, <http://www.privacy.gov.au/publications/PIA06.pdf>; August 2006 [accessed 27.02.08].

BBC News. UK families put on fraud alert. BBC News, <http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm>; 20 November 2007 [accessed 27.02.08].

Bennett CJ, Raab CD. The Governance of Privacy: policy instruments in global perspective. 2nd ed. Cambridge, Massachusetts: The MIT Press; 2006.

Canada, Ontario Access and Privacy Office. Privacy Impact Assessment: a user's guide. Toronto: Access and Privacy Office, <http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf>; 2001 [accessed 27.02.08].

Clarke R. A history of Privacy Impact Assessments, <http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html>; February 2004 [accessed 27.02.08].

Department of Health. Confidentiality: NHS code of practice. London: Department of Health, <http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253>; 2003 [accessed 27.02.08].

European Communities, Commission. Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. Official Journal of the European Communities 23 November 1995; L281:31.

House of Commons. Home Affairs Committee on Identity Cards. 3 February 2004.

House of Commons, Justice Committee. Protection of private data. First report of session 2007–2008. London: The Stationery Office Ltd.; 3 January 2008. HC 154, para 6.

ICO. The Identity Cards Bill – the Information Commissioner's perspective. December 2004.

ICO. The Identity Cards Bill – the Information Commissioner's concerns. October 2005.

ICO. Privacy Impact Assessments: international study of their application and effects. Wilmslow: Information Commissioner's Office, <http://www.ico.gov.uk/Home/about_us/research/data_protection.aspx>; December 2007a [accessed 27.02.08].

ICO. Privacy impact assessment handbook. Wilmslow: Information Commissioner's Office, <http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html>; December 2007b [accessed 27.02.08].

ICO. ICO launches CCTV code of practice consultation, <http://www.ico.gov.uk/upload/documents/pressreleases/2007/cctv_code_of_practice_consultation_final.pdf>; 2 August 2007c [accessed 27.02.08].

New Zealand Office of the Privacy Commissioner. Privacy impact assessment handbook. Office of the Privacy Commissioner, <http://www.privacy.org.nz/privacy-impact-assessment-handbook/>; March 2002 [accessed 27.02.08].

Northern Ireland Department of Finance and Personnel, Valuation and Lands Agency. Publication of capital value, <http://www.ratingreviewni.gov.uk/privacy_impact_assessment.pdf>; August 2006 [accessed 27.02.08].

Raab C, 6 P, Birch A, Copping M. Information sharing for children at risk: impacts on privacy, e-Care Programme, Leith, Health Department, Scottish Executive; 2004 [Publication: 23357].

Stewart B. Privacy impact assessments. Privacy Law & Policy Reporter, <http://www.austlii.edu.au/au/journals/PLPR/1996/39.html>, July 1996a;3(4):61–4 [accessed 27.02.08].

Stewart B. PIAs – an early warning system. Privacy Law & Policy Reporter, <http://www.austlii.edu.au/au/journals/PLPR/1996/65.html>, October/November 1996b;3(7):134–8 [accessed 27.02.08].

Stewart B. Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies. Privacy Law & Policy Reporter, <http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1999/8.html>, February 1999;5(8):147–9 [accessed 27.02.08].