Loughborough University

This item was submitted to Loughborough's Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/

Privacy Impact Assessments: the UK experience

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

[a]Department of Geography, Loughborough University, UK. Email: a.p.warren@lboro.ac.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

This paper builds on original work undertaken as part of a team of researchers into Privacy Impact Assessments (PIAs), defined as a systematic risk assessment tool that can be usefully integrated into decision-making processes. The team were commissioned by the UK Information Commissioner's Office (ICO) in June 2007 to develop a study of PIAs in overseas jurisdictions and a handbook to guide UK organisations through the PIA process. This research has subsequently attracted interest in the UK and overseas. PIAs are now mandatory for all UK central government departments. In this paper, the development of the project team's PIA methodology and subsequent user experiences led to a key project output, the PIA handbook. The handbook has become a significant part of the privacy 'toolkit' and has impacted on public policy. Some important lessons from PIAs conducted in the UK and overseas are identified. Finally, areas are outlined for further development.

1. Introduction

In July 2007, the UK data protection regulator, the Information Commissioner's Office (ICO), commissioned a team of researchers, led by Loughborough University, to assist its work in promoting the use of Privacy Impact Assessments (PIAs) in the UK[1]. The project remit was twofold:

1. To produce an international 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;
2. To draft a handbook for use by practitioners, to guide them through the PIA process in line with relevant UK legislation.

Although some reference will be made to findings from the international study, they have been discussed in greater detail elsewhere (Warren et al, 2008). Rather, this paper will focus on the project team's development of a PIA methodology, resulting in a handbook for practitioner guidance. However, before doing so, we wish to briefly place our work in context.

2. Context: Privacy Impact Assessments

PIAs have been defined as 'systematic risk assessment tool[s] that can be usefully integrated into decision-making processes' (Warren et al, 2008). They should aim to assess the entire project lifecycle from planning to operation (i.e. planning; requirements analysis; system design; and construction, implementation and operation of the new

---

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

system). Although the PIA concept has been in use since at least the 1970s (Clarke, 2004), PIAs as we recognise them began to be systematically developed in North America and Australia from the mid-1990s, representing a development of data protection or information privacy statutes that had been enacted in many Western democracies from the early 1970s onwards. The processes involved in conducting a PIA vary widely and include formats such as a handbook (e.g. Australia, 2006; New Zealand, 2002) and an eLearning Tool (e.g. Canada, 2003). They have been most commonly used by public sector organisations and have often been developed in conjunction with electronic government initiatives. PIAs have also been conducted in the private sector, although, in the absence of a mandate, the extent of activity is unknown. In this setting they are more likely to be carried out in circumstances where, firstly, companies have high-profile privacy expertise in the form of appointed Chief Privacy Officers, for example, TELUS and the Royal Bank of Canada (ICO, 2007a). Secondly, they are likely to be conducted in the context of private delivery of government schemes, for example, smart card applications, road-pricing and IT infrastructure projects.

After considering lessons from international experience, and taking into account the UK context, the project team determined that a UK PIA process should incorporate the following features:

1. Be a comprehensive risk analysis exercise

2. Be more process-oriented than output-oriented

3. Be integrated within existing management and business processes

4. Employ a screening tool

5. Provide flexibility of scale

6. Be transparent and accountable

7. Define organisational responsibilities

8. Provide for external review and approval (ICO 2007a: 34-36)

Due to restrictions on space, we only have time to consider a few of the above. However, it is worth noting that our research was made more timely by the high profile loss in November 2007 of personal data relating to child benefit records by HM Revenue and Customs. Following this incident, a Cabinet Office review was instigated. The ensuring report, *Data Handling Procedures in Government*, published in June 2008, mandated the use of PIAs in central government departments and called for PIAs to be built into the government's 'Gateway' reviews of ICT projects[2] (Cabinet Office, 2008). PIAs had thus become an important part of the privacy 'toolkit', informing UK public policy (Bennett and Raab, 2006).

---

[2] '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.

3. Privacy Impact Assessment handbook: a guide for practitioners

When drafting the PIA methodology in autumn 2007, the project team were sensitive to the fact that this was the first detailed PIA exercise in the UK and that, at the time, there had been no formal Parliamentary backing for the process. The team therefore aimed to produce a tool that organisations could integrate within their existing business processes. It was decided at an early stage that specifying a single, catch-all, PIA would not be appropriate as organisational projects vary enormously both in terms of scale – from the updating of a small business database to initiatives supporting the National Health Service's National Programme for IT – and privacy risk.

3.1 PIA Screening Tool
The project team recommended the use of a PIA screening tool, ensuring that organisations were 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 were undertaking. The screening tool allows practitioners to conduct a limited preliminary evaluation, establishing the extent to which their organisation needed to invest in the PIA process. An outline is presented in Figure 1.

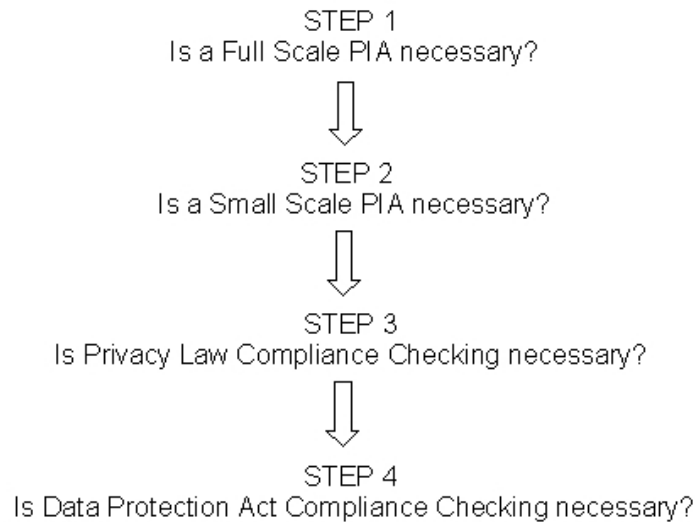***Insert Figure 1 [separate attachment] here***

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 perceived as a matter of strategic significance rather than just an administrative add-on.

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 'Data'. 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.

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 questions for Steps 1 and 2 are listed side by side in Table 1 for comparative purposes.

```
                    STEP 1
           Is a Full Scale PIA necessary?

                      ⇩

                    STEP 2
          Is a Small Scale PIA necessary?

                      ⇩

                    STEP 3
      Is Privacy Law Compliance Checking necessary?

                      ⇩

                    STEP 4
   Is Data Protection Act Compliance Checking necessary?
```

Table 1

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.

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 see whether laws other than the UK Data Protection Act are relevant (law of confidence, Human Rights Act, Regulation of Investigatory Powers Act, Privacy and Electronic Communications Regulations);
ii. A simple set of tests to establish whether the provisions of the UK Data Protection Act itself are applicable.

4. User engagement and experiences

The handbook (ICO, 2007b) was launched in December 2007. Since that period, a large number of organisations have conducted PIAs, a trend hastened by the element of compulsion introduced following the Cabinet Office review (Cabinet Office, 2008). As there is no requirement for organisations in the UK to inform the ICO that they are conducting PIAs, there is no way of gauging the total number underway. The difficulty in quantifying PIA activity is compounded by the fact that, at the time of writing, very few UK PIA reports exist in the public domain. Table 2 highlights two recently published reports. They were conducted by staff within the organisations and made use of the methodology drafted by the project team.

Insert Table 2 here

UK PIAs have also been outsourced to external consultants. Some examples are outlined in Table 3, below.

Insert Table 3 here

External consultants often bring considerable experience to the PIA process, lending impartiality to the process. They can offer frank advice when initiatives are deemed to be unwise or ill-conceived, and tend to have greater expertise and familiarity with relevant legislation (ICO, 2007a). Yet, there are disadvantages. Smaller organisations may find them prohibitively expensive. Moreover, there is scepticism about consultants using 'cookie cutter' PIAs whereby the same templates are used for vastly different clients (ICO, 2007a). Conversely, there is a risk that organisations will use the external consultants to 'legitimise' controversial projects or applications. For example, a PIA conducted in 2008 by 80/20 Thinking Ltd for Phorm, a company specialising in targeted online advertising, generated considerable debate among privacy experts, and in sections of the mainstream media, about the motivations behind the exercise (refer, for example to: Arthur, 2008; BBC, 2008).

Finally, although the extent of UK user engagement is difficult to determine, our methodology has attracted interest overseas, notably from national and transnational public authorities[3]. The Netherlands Data Protection Authority (*College Bescherming Persoonsgegevens*) has launched a feasibility study into using the ICO's handbook in the Dutch context, whilst the Norwegian Data Inspectorate (*Datatilsynet*) has expressed an interest in the ICO's PIA methodology. At the same time, the Mexican government approached the ICO to conduct a PIA relating to the management of their national health records. Finally, the European Data Protection Supervisor recommended in March 2008 that 'exhaustive privacy impact assessment[s]' should be conducted on proposed EU border management systems. Our methodology was referenced in his comments (EDPS, 2008: 4).

5. Key lessons learnt

A number of lessons have been learnt from both our background research into PIAs conducted overseas and from the experiences of consultants using our methodology. Firstly, some lessons identified from earlier, overseas, experiences. We found that, in order to be effective, PIAs:

- Need to be accountable. The PIA reports should be published or otherwise made available;
- Need to be prospective. Privacy risk needs to be identified *before* systems are put in place
- Need to refer to entire process of assessment of privacy risk, rather than just the end-product or statement. A final report, if published, often offers deceptive impression of the nature, scope and depth of the assessment exercise.

---

[3] Information in this paragraph has been supplied by officials at the UK ICO.

- Need to have potential to alter proposed initiatives; should not be mechanical 'tick box' exercise or an exercise in legitimation rather than in risk assessment (ICO, 2007a: vi-vii).

Secondly, we wish to highlight some difficulties experienced by organisations considering conducting a PIA[4]. From the outset, those carrying out PIAs encountered internal stakeholder resistance. Our handbook recommends that stakeholder analysis is embedded into the PIA process[5], but it was found that project managers often perceived PIAs to be a burden and public relations managers were often very wary of engagement of external stakeholders or publication of the process. In addition, security officers sometimes considered PIAs to be a threat to their expertise and consequently their position in the organisation. Moreover, there was reluctance to engage amongst external stakeholders such as independent experts, regulators, civil society groups, professional bodies and charities. It was noted that the ICO itself did not have resources to validate PIAs and that civil society groups, in particular, were often too time-pressured - and also lacked the resources - to contribute to the process.

6. Conclusion: areas for further development

In spite of the research conducted by the project team in 2007 and the significant policy developments in this field, particularly in the UK, there appears to have been little academic interest in PIAs (Clarke, 2009). One exception to this has been in the field of computer science, where collaborative research has been undertaken with industry to assess the extent to which PIA principles could be integrated into an automated decision support tool to determine which information can be shared in a social care setting (Harbird et al, 2008). In the current economic climate, with public rationalisation firmly on the political agenda, the integration of the PIA process with technologies represents an attractive policy option. A second area of development is the promotion and evaluation of private sector use of PIAs. Although this does present difficulties, not least due to proprietary issues (ICO, 2007a: 14), it would be interesting to gauge the extent to which different strategies can be used for performing PIAs in key commercial sectors, for example, finance, IT, banking and pharmaceuticals.

Whilst the PIA is a policy tool with a genesis extending back some decades (Clarke, 2004; ICO, 2007a), it is only in the last eighteen months that it has started to impact on UK policy. Therefore, plenty of scope exists for further development of PIAs, for example, through: identifying linkages between PIAs and policymaking; improved stakeholder engagement; greater use of technologies; and possible partnerships with the private sector.

---

[4] Information in this paragraph is derived from a presentation given by Toby Stevens, Director of Enterprise Privacy Group, to an ESRC workshop, *Assessing Privacy Impact*, held in London in June 2009. URL: http://www.esrc.ac.uk/ESRCInfoCentre/about/CI/events/esrcseminar/privacyimpact.aspx

[5] PIA process comprises 5 phases: Preliminary; Preparation; Consultation and Analysis; Documentation; Review and Audit.

Acknowledgements

Bibliography

Arthur, C. (2008) Simon Davies (of Privacy International, and 80/20 Thinking) on Phorm. Technology Blog, *The Guardian*, 20 March http://www.guardian.co.uk/technology/blog/2008/mar/20/simondaviesofprivacyintern [accessed 16/10/09]

Australia (2006). Office of the Federal Privacy Commissioner. Privacy Impact Assessment Guide. Office of the Privacy Commissioner, Sydney.

BBC (2008) Phorm needs 'better protection', *BBC News*, 18 March http://news.bbc.co.uk/1/hi/technology/7303426.stm [accessed 16/10/09]

Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press).

Cabinet Office (2008). *Data Handling Procedures in Government: Final Report.* London: Cabinet Office.

Canada (2003). Treasury Board of Canada Secretariat. *Privacy Impact Assessment (PIA) e-learning tool*. Treasury Board Secretariat, Ottawa, October, at http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp [accessed 16/10/09]

Clarke R. (2004) A history of Privacy Impact Assessments, <http://www.rogerclarke.com/DV/PIAHist.html#OrigT>; February [accessed 16/10/09].

Clarke, R. (2009) Privacy impact assessment: Its origins and development, *Computer Law and Security Review*, 25 (2): 123-135.

European Data Protection Supervisor (EDPS) (2008) *Preliminary Comments of the European Data Protection Supervisor on […]* 2008 http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf [accessed 16/10/09]

Harbird, R., Finkelstein, A., Hailes, S., McKinney, E. and Jeyarajah-Dent, R. (2008) PRAIS - PRivacy impact Analysis for Information Sharing. In: *Healthcare Conference HC2008: An invitation to the future*, 21-23 April, 2008, Harrogate, UK.

ICO (2007a). *Privacy Impact Assessments: international study of their application and effects*. Wilmslow: Information Commissioner's Office.

ICO (2007b). *Privacy Impact Assessment Handbook.* Wilmslow: Information Commissioner's Office.

ICO (2009). *Privacy Impact Assessment Handbook. Version 2.0.* Wilmslow: Information Commissioner's Office.

New Zealand (2002). Office of the Privacy Commissioner. *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner.

Warren, A.P., Bayley, R., Bennett, C., Charlesworth, A., Clarke, R. and Oppenheim, C. (2008). Privacy Impact Assessments: international experience as a basis for UK guidance. *Computer Law and Security Report*, 24 (3): 233-242.

Step 1: Criteria for full-scale PIA	Step 2: Criteria for small-scale PIA
Technology	
Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?	Does the project involve new or inherently privacy-invasive technologies?
Justification	
No questions under this heading	Is the justification for the new data-handling unclear or unpublished?
Identity	
Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?	Does the project involve an additional use of an existing identifier?
Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	Does the project involve use of a new identifier for multiple purposes?
-	Does the project involve new or substantially change identity authentication requirements that may be intrusive or onerous?
Multiple organisations	
Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?	*No questions under this heading*
Data	
Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?	Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?
Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?	Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?
Does the project involve new or significantly changed handling of personal data about a large number of individuals?	Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?
Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	
Data handling	
No questions under this heading	Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?
	Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?
	Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?
	Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

	Does the project involve new or changed data retention arrangements that may be unclear or extensive?
	Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?
Exemptions and exceptions	
Does the project relate to data processing which is in anyway exempt from legislative privacy protections?	Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?
Does the project's justification include significant contributions to public security measures?	
Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	

Table 1: PIA Screening Tool questions (ICO, 2009)

Organisation	Type of Privacy Impact Assessed	Type of PIA conducted
UK Border Agency (2009)	Exchange of fingerprint information with immigration authorities in Australia, Canada, United States and New Zealand	Small-scale
National Policing Improvement Agency (2009)	Electronic exchange of police intelligence across England and Wales via the Police National Database.	Full-scale

Table 2: UK public sector PIA reports in the public domain

Organisation	Type of Privacy Impact Assessed	Consultancy employed
Aegate (Pharmaceutical authentication services)	Use of RFID technologies to authenticate prescription pharmaceuticals at the point of sale	Enterprise Privacy Group
Department for Transport	National time-distance-place road pricing policy[6]	Enterprise Privacy Group
Phorm Inc	Behavioural targeted advertising	80/20 Thinking Ltd

Table 3: Examples of PIAs outsourced to consultants

---

[6] In this system of road pricing vehicles are charged based on when, where, and how much they drive.