The state of the art in privacy impact assessment

David Wright[1]
Trilateral Research & Consulting, London

Abstract

This paper presents some findings from the PIAF project. PIAF is the acronym for a Privacy Impact Assessment Framework. The project, which began in January 2011, is being undertaken for the European Commission's Directorate General Justice. The first deliverable was completed in September. The paper provides some background on privacy impact assessment, identifies some of its benefits and elements that can be used in construction of a state-of-the-art PIA methodology.

Introduction

The European Commission is expected to issue its proposed revisions to the data protection framework later this year. It signalled some of the changes we can expect in its Communication of 4 November 2010. One of the changes concerns "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data is being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms, or procedures, including profiling or video surveillance."[2]

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

We have completed work on our first deliverable which can be found on the consortium's website.[3] The first deliverable reviews PIA policies and practices in the six above-mentioned countries plus Ireland as well as 10 case studies of PIA reports. The report also has a set of conclusions which identifies the benefits to organisations of undertaking privacy impact assessments and some of the best elements we have found in our review of existing policies and practices.

[1] The views expressed in this paper are those of the author alone, and are in no way intended to reflect those of the PIAF consortium. Comments on this paper are welcome and can be sent to david.wright@trilateralresearch.com

[2] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[3] www.piafproject.eu

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

Definition

There are various definitions of PIA, but we define a privacy impact assessment as a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a *process* which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed[4].

Although privacy impact assessment has been used in Australia, Canada, New Zealand and the United States since the mid-1990s, the methodology is a relatively new phenomenon in Europe. The UK Information Commissioner's Office published its PIA Handbook in December 2007 and a revised version in June 2009. It became the first country in Europe to publish a PIA guidance. Ireland became the second with the publication of its PIA guidance in December 2010.[5]

These two guidance documents, like those in Australia, Canada, New Zealand and the US, have some good points but also some shortcomings. Thus, Europe has the opportunity to build on the experience of others to develop a state-of-the-art PIA policy and practice. It can also take into account the RFID PIA Framework which was developed by industry and approved by the Article 29 Working Party in February 2011.[6]

While a privacy impact assessment is a methodology for identifying risks to privacy posed by any new project, product, service, technology, system, programme, policy or other initiative and devising solutions to avoid or mitigate those risks, it also offers several important benefits to organisations, their employees, contractors, customers, citizens and regulators. Among them are the following:

Benefits

A PIA has often been described as an early warning system. It provides a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments. The costs of fixing a project (using the term in its widest sense) at the planning stage will be a fraction of those incurred later on. If the privacy impacts are unacceptable, the project may even have to be cancelled altogether. Thus, a PIA helps reduce costs in management time, legal expenses and potential media or public concern

[4] The word "project" is used in this paper in its widest sense, to include any technology, product, service, programme, policy or initiative that may impact upon privacy.

[5] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care,* Dublin, December 2010. http://www.hiqa.ie/resource-centre/professionals

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

by considering privacy issues early.It helps an organisation to avoid costly or embarrassing privacy mistakes.

Although a PIA should be more than simply a compliance check, it does nevertheless enable an organisation to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation. In the event of an unavoidable privacy risk or breach occurring, the PIA report can provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.[7]

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions about the project. A PIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers.A PIA functions as a credible source of information.Itenables an organisation to learn about the privacy pitfalls of a project, rather than having its critics or competitors point them out.A PIA assists in anticipating and responding to the public's privacy concerns.

A PIA can help an organisation to gain the public's trust and confidence that privacy has been built into the design of a project, technology or service. Trust is built on transparency, and a PIA is a disciplined process that promotes open communications, common understanding and transparency. An organisation that undertakes a PIA appropriately demonstrates that the privacy of individuals is a priority for their organisation. It affirms that an organisation has addressed privacy issues and has taken reasonable steps to provide an adequate level of privacy protection.

An organisation that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them to do so too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that might damage the organisation. It is a way to affirm the organisation's values.

A proper PIA also demonstrates to an organisation's customers and/or citizens that it respects their privacy and is responsive to their concerns. Customers or citizens are more likely to trust an organisation that performs a PIA than one that does not. They are more likely to take their business to an organisation they can trust than one they don't.

We assume regulators are likely to be more sympathetic towards organisations that undertake PIAs than those that do not.

Elements in good policy and practice

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

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

Roles – Who initiates a PIA and who approves it?

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

Threshold analysis – Is a PIA necessary?

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

Clarity for whom the PIA is prepared

Those undertaking a PIA should be clear for whom they are preparing it – e.g., for senior management, for the regulator, for stakeholders, for the public.

Process

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

Scale and scope of the PIA

The scale and scope of a PIA should generally be in line with the scale and scope of a project. A more elaborate PIA – and more resources for carrying it out – will be needed for a complex project.

PIA starts early

The sooner a PIA starts, the better. It should start early enough so that it can influence the design of a project. It is useless if it is undertaken after all the decisions have been made.

Privacy, not just data protection

The Commission has used the term "data protection impact assessment", but we hope that it will drop that terminology in favour of "privacy impact assessment". PIA is the terminology that has been used by all other countries, and we think that using the term DPIA risks sending the wrong message to organisations. Informational privacy is only one type of privacy. Roger Clarke and others have identified other types of privacy that are also important – privacy of the body, privacy of communications, privacy of location, privacy of behaviour. If industry and governments think the Commission's main or only concern is with data protection, informational privacy, then these other forms of privacy could be brushed aside.

PIA as part of risk management

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

Questions to identify risks and solutions

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

PIAs are only as good as the processes that support them

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

- Programs in place to inform staff and other stakeholders of the policy's objectives and requirements;
- Formally defined program responsibilities and accountabilities;
- The existence of a system to effectively report all new initiatives that may require a PIA;
- The existence of a body composed of senior personnel charged with reviewing and approving PIA candidates;
- The existence of an effective system of monitoringcompliance with the PIA policy;
- Adequate resources committed to support the organisation's obligations under the policy.[8]

Training and raising awareness of employees

Coupled with the above, and to embed PIA within its culture and practices, the organisation needs to install an ongoing employee awareness program, effectively raising the profile of PIAs and regulatory requirements for their performance with program managers and new hires. Creating general awareness of the policy requirements respecting privacy is often the first step towards ensuring that program managers fully consider the privacy impacts of their plans and priorities at the time an initiative is conceived.[9]

Mandatory PIAs

Undoubtedly, a contentious issue is whether PIAs should be mandatory, as the Commission indicates in its Communication. PIA is already mandatory in Canada, the UK and the US, at least for government agencies. They are also mandatory for the private sector in certain other

[8] Office of the Privacy Commissioner of Canada, *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report of the Privacy Commissioner of Canada, Ottawa, 2007, p. 9.
[9] OPC, 2007, p. 17.

instances, for example, involving health care or biometrics. There is a strong case for mandatory PIA, as the Commission indicates, in projects involving sensitive data, surveillance and profiling. Unless they are mandatory, many organisations may not undertake them even though their projects, technologies or services have serious privacy impacts. Nevertheless, the logistics of mandatory PIA are not so straightforward. Mandatory PIA would need to be complemented by audits and, desirably, publication and stakeholder engagement.[10]

Engaging stakeholders

The ICO PIA Handbook puts a strong emphasis stakeholder engagement and consultation. The ICO is of the view that if a PIA is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It therefore recommends that stakeholder perspectives are considered.[11] Australia's PIA Guide makes a similar point. It says "Consultation with key stakeholders is basic to the PIA process." It adds that

> A PIA should always consider community privacy attitudes and expectations. Affected individuals are likely to be key stakeholders, so wider public consultation is important, particularly where a lot of personal information is being handled or where sensitive information is involved. Public consultation also adds to community awareness about the project and can increase confidence in the way the project (and the organisation) is handling personal information.

Recommendations and an action plan

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

Publication of the PIA report

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

Third party audits and monitoring implementation

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

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

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

including from the perspective of the organisation itself. Audits lead to improvements in PIA practice.

PIAs, state security and commercially sensitive issues

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

Accountability

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

Tying PIAs to budget submissions

In Canada and the US, PIAs are tied to budget submissions. In Canada, government institutions must complete and forward a PIA to the Treasury Board of Canada Secretariat to accompany submissions for funding new programs and projects, and in the US, government agencies must include a PIA with submissions to the Office of Management Budget.

A central registry of PIAs

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

Conclusion

Our review of PIA methodologies and reports show that there are similarities as well as differences among the seven countries. Europe can benefit from their experience by drawing upon their best elements to create its own state-of-the-art PIA policy and practice. This paper has presented some of the elements that can be used to construct an optimised PIA.

For further information:

Wright, David, “Should privacy impact assessments be mandatory?”,*Communications of the ACM*, Vol. 54, No. 8, August 2011. http://cacm.acm.org/magazines/2011/8

PIAF Deliverable D1, September 2011. www.piafproject.eu

Wright, David, and Paul De Hert (eds.), Privacy Impact Assessment, Springer, Dordrecht, 2012 [forthcoming]