Innovation: The European Journal of Social Science Research, 2013
Vol. 26, Nos. 1–2, 161–180, http://dx.doi.org/10.1080/13511610.2013.761748

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

Evaluating privacy impact assessments

Kush Wadhwa* and Rowena Rodrigues

Trilateral Research & Consulting, London, UK

(*Received 28 December 2011; final version received 11 December 2012*)

Privacy impact assessments (PIAs) are emerging as an important privacy management tool for public and private sector organizations. However, a key concern of PIA policy and practice is the lack of follow-up and means to evaluate its conduct at different levels, particularly so that different stakeholders can make sense of PIA practice as evidenced in PIA reports. This article first outlines the evaluation criteria established under the EU Privacy Impact Assessment Framework project and attempts to find the best means of extending their application to help assess PIAs, based on good practice.

Keywords: privacy impact assessments; PIAs; PIA evaluation; PIAF

Introduction

Privacy impact assessment (PIA) is emerging as a critical privacy management tool for public and private sector organizations alike. Several countries mandate their use for public sector projects to deploy new systems, and the proposed data protection regulation from the European Commission mandates PIAs where sensitive data are processed. The European Parliament Resolution on a comprehensive approach on personal data protection in the European Union (European Parliament 2011) "Considers it essential to make Privacy Impact Assessments mandatory in order to identify privacy risks, foresee problems, and bring forward proactive solutions". The Privacy and Data Protection Impact Assessment Framework for Radio Frequency Identification (RFID) applications (European Commission 2011) also illustrates the importance of PIAs in privacy and data protection.

According to Wright and De Hert (2012a), a PIA is a "methodology for assessing the impacts on privacy of a project, policy, program, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts". PIAs, which are contemporary privacy protection mechanisms, surfaced initially and developed from the mid-1990s in Australia, Canada, Hong Kong, New Zealand and the United States. They have their roots in environmental impact assessments and social impact assessments (SIAs).[1]

*Corresponding author. Email: kush.wadhwa@trilateralresearch.com

The UK Information Commissioner's PIA Handbook (2009) outlines why PIAs are required:

- to identify and manage privacy risks (signifying good governance and good business practice);
- to avoid unnecessary costs (of problems discovered at later stages);
- to avoid inadequate solutions implemented at later stages;
- to avoid loss of trust and reputation by addressing concerns;
- to inform the organization's communications strategy (through understanding perspectives); and
- to meet and exceed legal requirements.

Currently, in locations where PIAs are required, or required under particular circumstances – Australia (Office of the Privacy Commissioner 2010), Canada (Treasury Board of Canada Secretariat 2002), Ireland (Health Information and Quality Authority 2010), New Zealand (Office of the Privacy Commissioner 2007), UK (ICO 2009), United States (Office of Management and Budget 2003) – they are intended to be performed early in the project life cycle so that there is an opportunity to have an impact on the implementation of the project, enhancing privacy and reducing the myriad privacy and data protection related risks. However, although standards for the PIA process have taken root at the government level in some countries, their uptake is not uniform, nor is the actual implementation of the process.

One of the key concerns of PIA policy and practice is the lack of follow-up and means to evaluate its conduct at different levels, particularly for different stakeholders to make sense of PIA practice, as evidenced in PIA reports. This article first outlines the evaluation criteria established under the EU Privacy Impact Assessment Framework (PIAF) project[2] and tries to find the best means of extending their application to help assess PIAs, based on good practice.

The PIAF criteria

Background

The PIAF report (Wright et al. 2011), reviewing the PIA methodologies of seven countries, presented the most complete compendium and analysis of PIA policies and practices yet compiled and published. It reviewed and compared PIA methodologies (policies and practice) in Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and the United States. The study uniquely presented and applied a list of criteria for evaluating the effectiveness of PIAs based on PIA reports.

Statement of the criteria

The PIAF report used the following criteria to measure the effectiveness of PIA reports and, through them, to assess the overall PIA process:

(1) early initiation of PIA;
(2) identification of who conducted the PIA;
(3) description of the project to be assessed, its purpose and any relevant contextual information;

(4) mapping of information flows (i.e. how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained);
(5) checking of the project's compliance against relevant legislation;
(6) identification of the risks to or impacts on privacy;
(7) identification of solutions or options for avoiding or mitigating the risks;
(8) recommendations;
(9) publication;
(10) stakeholder consultation.

These criteria guided the evaluation of 10 PIA reports (two reports per country) from Australia, Canada, New Zealand, UK and the United States. The analysis revealed that the PIA reports commonly contained, in some form and to varying degree, the following: a project description, a statement of purpose, relevant contextual information, identification of privacy risks and impacts, and identification of solutions or options for risk avoidance and mitigation. In relation to the other evaluation criteria, there were significant differences in practice. PIA reports vary as much between jurisdictions as within.

Employing the criteria for PIA enhancement

This paper intends to take the criteria and lessons learnt from the first PIAF report and seeks to apply them to help enhance the effectiveness of PIAs.

The need to enhance PIAs

PIAs, as currently conducted, although a positive development, have a lot of room for improvement. Wright (2011) states

> Making privacy impact assessments mandatory is not the end of the story. Audits and metrics are needed to make sure that PIAs are actually carried out and properly so and to determine if improvements to the process can be made.

One of the more severe criticisms is that PIAs often resemble no more than window dressing or represent "another ritualised hurdle to jump over" (Marx 2012). In this respect, one of the significant challenges is the lack of post-PIA evaluation. The effectiveness of PIAs needs enhancement. This can happen only if the PIA process is dynamic and PIAs have some sort of follow-up. One means of achieving this is by evaluating PIA reports. However, currently, there is no easy, standardized means of conducting this evaluation. To achieve this end, we propose a PIA Evaluation and Grading System (PEGS).

Related work

There are a number of PIA risk assessment tools, which help organizations assess privacy risks and facilitate the PIA process (note, as compared with PEGS, which evaluates the actual PIA process post facto, although it may be also employed to guide the PIA process). Among privacy risk assessment tools are: the AIPCA/CICA privacy risk assessment tool; the Security and Privacy Impact Assessment (SPIA)

Tool of the University of Pennsylvania; the GS1 RFID Privacy Impact Assessment (PIA) tool; the Vienna University intelligentPIA tool for RFID applications; and the Privacy Impact Assessment Tool for Cloud Computing proposed by Tancock, Pearson, and Charlesworth (2010). We briefly summarize (for full and up to date information, the reader should refer to the respective websites) and then assess each of these tools against the following yardsticks:

Operational usability	Is the tool itself simple and intuitive to use with a minimum need for training?
Contextual usability	Are the questions asked/examined when using the tool easy to understand with a minimum need for training?
Applicability	Is the tool equally applicable to a broad range of applications and technologies?
Thoroughness	Are the questions examined in using the tool broad/sufficiently detailed in scope?
Accessibility	Is the tool easy to find on the Internet? Is it costly to gain access to the tool?
Privacy focus	Is the tool focused only on privacy-related issues, or is it a subset of a larger evaluation process?

We next analyze the different PIA tools, outline their advantages and disadvantages and comparatively illustrate how they fare against the above listed yardsticks.

The AICPA/CICA privacy risk assessment tool

The Privacy Risk Assessment Tool developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) aims to help organizations perform privacy risk assessments. The tool, designed in spreadsheet form, is based on the 10 principles and 73 criteria contained in the AICPA/CICA Generally Accepted Privacy Principles (GAPP).[3] The tool comprises a Scoring Input Template (10 separate files with unique names to accommodate 10 assessors) and a Scoring Summary. This model uses a three-point scoring system (i.e. 2 = low risk, 5 = medium risk or 8 = high risk) to evaluate the GAPP criteria against the following: likelihood of control failure, business impact and mitigation/prevention costs. After the scoring is complete in the individual assessment templates, the tool summarizes the scoring for all GAPP criteria under the relevant GAPP principle and graphically illustrates the results.

The AICPA/CICA Privacy risk assessment tool is comprehensive and has the ability to accommodate multiple assessors. The accompanying guidance is good. It is a good initial assessment measure. However, although intended to be user-friendly and intuitive, it is slightly complex. It is designed for use by “privacy professionals who have a good understanding of privacy laws and regulations, privacy best practices, business operations, risk assessments, and current privacy practices and controls within the organization” (AICPA/CICA 2010).

The SPIA risk assessment tool of the University of Pennsylvania

The University of Pennsylvania has a SPIA risk assessment tool (also in spreadsheet format) for its schools/centers that “offers suggestions for what safeguards may be appropriate in order to mitigate the most common threats and provides a reporting template to help synthesize the learning and proposed changes that result from the SPIA process" (University of Pennsylvania 2007). The tool is designed as a "roadmap to help organizations identify areas of risk and select appropriate strategies and timeframes to mitigate those risks" (University of Pennsylvania 2007). The tool enables organizations to take probability rankings and threat consequences and automatically score risk into categories of "High", "Significant", "Moderate" or "Low". Threats (security and privacy) are broadly identified. In its scoring of threats, the tool employs a six-point scale:

0 = Threat does not apply to this application/database.
1 = Rare – the event would only occur under exceptional circumstances.
2 = Unlikely – the event could occur at some time, but probably will not.
3 = Moderate – the event should occur at some time.
4 = Likely – the event will probably occur at some time.
5 = Almost certain – the event is expected to occur in most circumstances.

After the current probability of each threat is scored against each application/database, the current potential consequences of the threat being realized are evaluated on a scale of 0–5 (0 = threat is not applicable, 1 = insignificant, 2 = minor, 3 = moderate, 4 = major, 5 = disastrous). The results then help in the re-evaluation of each threat, this time taking into account planned risk mitigation safeguards to obtain a revised risk value.

The SPIA risk assessment tool is versatile and adaptable enough to include additional threats. It is designed to be objective. On the downside, the tool is rather overwhelming at first glance, consisting of several disconnected spreadsheets to drive the assessment process. Moreover, the SPIA tool looks at security risks as well as privacy impacts, requiring much broader analysis and risking the possibility of losing sight of privacy issues amongst the myriad security issues that may need to be addressed.

GS1 EPC/RFID PIA tool

GS1, an international association dedicated to the design and implementation of supply chain standards, has implemented a PIA tool for use in the design phase of RFID applications. The tool aims to help large and small-scale enterprises evaluate whether an application meets "consumer privacy expectations" (GS1 2012). Similar to the SPIA tool, it uses spreadsheets with detailed screens. The tool, according to GS1, is designed to

- rapidly perform *a comprehensive assessment of privacy risks* of any new EPC/RFID implementation within your company;
- identify *privacy controls* to be built in at the early stages of the specification or development process;
- comply with the *European Commission's RFID Recommendation* and best practices on privacy and data protection, including the EPC Privacy Guidelines.

The GS1 EPC/RFID PIA tool has three parts: the Assessment Setup; the Initial Assessment; and the Detailed Assessment. In the Assessment Setup, the RFID

Application Operator provides general information about the organization, the RFID application and its operations. The Initial Assessment determines the need for a detailed PIA and to complete this, the RFID Application Operator answers four questions that determine whether the assessment is complete or whether level 1, 2 or 3 detailed assessments are required. The detailed assessment addresses predefined specific risks, the likelihood of their occurrence, the impacts of the risk and risk mitigation controls. A series of questions helps judge the levels of privacy risks (likelihood and impact) and controls. The effectiveness of controls is evaluated on a scale of 1–5 (least to most). A control rated less than 3 calls for detailed explanation of the control.

The Impact is multiplied by the Likelihood and subtracted from the Controls to attain the scoring. If a risk has no controls, a penalty is assigned. The scores of all controls are tallied and totalled against each risk, and scores from all risks are totalled and tallied for the overall assessment score.

The GS1 EPC/RFID PIA Tool has its advantages. It is available in two Excel versions (2007/2010 and 2003). GS1 recommends that generated reports are made available to data protection authorities and thus advocates the principle of oversight. The tool is simpler than the AICPA/CICA and the SPIA tools. One of its disadvantages is that it is incompatible with older computers. The tool is tailored to RFID implementations rather than a broader range of systems and applications that could be privacy intrusive.

The intelligentPIA tool for RFID applications

The intelligentPIA (iPIA) tool is a PIA for RFID applications.[4] The tool, designed by the Institute for Management Information Systems, Vienna University, is an open source application written in PHP and JavaScript using jQuery UI.

There are eight steps in the assessment process: characterization of the application; initial analysis; definition of privacy targets; evaluation of degree of protection demand for each privacy target; identification of threats; identification and recommendation of controls; consolidated view of controls; assessment and documentation of residual risks.

First, the RFID application must be characterized. This involves describing "scenarios and use cases, systems and system components, interfaces, data flows and involved parties", and identifies "the scope, boundaries and assets (resources and information) that need to be protected" (Institute for Management Information Systems 2012). Next, an initial analysis (based on a decision tree taken from the official RFID PIA framework) follows to determine the type of PIA required; that is, full-scale, small-scale or none. The tool outlines privacy targets next. The tool lists 16 privacy targets derived from the European Data Protection Directive 95/46/EC (European Parliament and the Council 1995.). Additional targets may be added, as required. The tool then evaluates the degree of protection for each target based on three demand categories: low, scored at 1; medium scored at 2; and high, scored 3.

The next step is identifying threats for each privacy target. The tool lists 60 such likely threats and enables the inclusion of additional threats. Controls, either of technical (access control mechanisms, authentication mechanisms and encryption methods) or non-technical nature (management and operational controls as well as accountability measures, policies or operational procedures and information measures taken with regard to data subjects), are to be identified next. The intelligentPIA tool offers 27 controls, with provision to add additional controls. The tool presents the identified controls in a consolidated, tabular form, allowing one to judge if the control has been implemented, planned or unplanned. The last step is an assessment and documentation of residual risks. The tool generates the report as a PDF file.

The intelligentPIA tool is a simple and systematic tool. However, its scope is limited to RFID applications.

The privacy impact assessment tool for cloud computing proposed by Tancock, Pearson and Charlesworth

Tancock, Pearson, and Charlesworth (2010) present a design for a PIA tool for cloud computing. The tool (not implemented at time of this assessment) addresses "the complexity of privacy compliance requirements for organizations (both public and private sector), by highlighting privacy risks and compliance issues for individuals within the organization who are not experts in privacy and security, so they can identify solutions in a given situation" (Tancock, Pearson, and Charlesworth 2010). The tool is expected to work as a "service accessible from a web browser, using a Software as a Service (SaaS) model, in which external organizations can ask to use that service (probably on a pay-per-use basis), in order to generate PIA reports based on their input, as required. In this model, security mechanisms are used in order to protect any confidential information that is transferred or stored by the service" (Tancock, Pearson, and Charlesworth 2010).

This PIA tool is envisaged as a decision support system (DSS) with a knowledge base (KB) maintained on an ongoing basis by privacy experts. The tool comprises templated questions and answers based on different contexts. After use, a detailed output report is generated including the risk levels of privacy domains.

The advantages are that the tool is designed for use in both full-scale and small-scale PIA. It is thus efficiently tailored. Its web-based nature eliminates the cumbersomeness of using spreadsheet-based solutions. It can be run at different stages of a project's development process lifetime, each time producing output and advice appropriate to that stage.

The disadvantages are that this tool might prove expensive to implement and maintain. It is tailored to the cloud computing environment and is not adapted for broader application.

Table 1 lists the advantages and disadvantages of how the tools fare comparatively against the yardsticks outlined previously. The analysis shows that most of the reviewed existing PIA tools are spreadsheet-based applications, which are quick, easy to access, easily available and affordable. Web-based applications, on the other hand, require more resources, and are more expensive to deploy and maintain.

The PIA tools examined in Table 1 all facilitate the PIA process. They help organizations comply with privacy requirements. The output of these PIA tools are PIA reports that embody an organization's approach to privacy for a specific application. None of the tools, however, provides a means of evaluating this output. This evaluation, we suggest, is an important element of accountability.

Table 1. Comparative analysis of selected PIA tools.

		The AICPA/CICA privacy risk assessment tool	The SPIA tool	GS1 EPC/RFID PIA Tool	iPIA tool	Cloud computing PIA tool
Operational usability	Is the tool itself simple and intuitive to use with a minimum need for training?	No	No	Yes	Yes	Intention expressed
Contextual usability	Are the questions asked/criteria examined when using the tool easy to understand with a minimum need for training?	No	No	Yes	Yes	Unclear (tool not deployed)
Applicability	Is the tool equally applicable to a broad range of applications and technologies?	Yes	Yes	No	No	No
Thoroughness	Are the questions examined in using the tool broad/sufficiently detailed in scope?	Yes	Yes	Yes	Yes	Unclear (tool not deployed)
Accessibility	Is the tool easy to find on the Internet? Is it costly to gain access to the tool?	Easy to find/free	Easy to find/free	Easy to find/free	Easy to find/free	Not implemented yet (intended to be a pay for access tool)
Privacy focus	Is the tool focused only on privacy-related issues, or is it a subset of a larger evaluation process?	Privacy focussed	Security and privacy focussed	Privacy focussed	Privacy focussed	Privacy focussed

PEGS

How might we add value to the work of these PIA tools? We examine this next and propose one specific means of doing so. The PIA Evaluation and Grading System, or PEGS, is primarily a PIA enhancement tool designed to make the PIA process more effective through the provision of a useful and efficient means of evaluating and grading PIA reports. This evaluation and grading has both a broad and specific purpose. The broad and overarching purpose is to enhance the effectiveness of PIAs with the help of the rich experience of PIA policy and practice as evidenced in the PIAF project. The specific, underlying purpose is to provide a practical means of determining how a PIA fares in relation to other PIAs.

PIA guidance has been criticized for being too burdensome, cumbersome and contrary to the "KISS principle, that is, keep it simple stupid" (Flaherty 2000). Therefore, we need a simple, convenient means of embodying the PIA evaluation criteria identified before. At the same time, we need to expand the criteria to include the whole gamut of the PIA process. Moreover, the evaluation means need to be adaptable, given that PIA requirements are not universal or might change with the passage of time (i.e. to maintain the dynamism of PIAs).

Checklists are a widely used methodology in environmental (Morgan 1999), health (Kemm, Parry, and Palmer 2004) and regulatory impact assessment (Radaelli and de Francesco 2010). Checklists are popular in privacy assessment too, as evident in the cases of Australia (Office of the Privacy Commissioner 2006), Canada (OCIPO 2010; Treasury Board of Canada Secretariat 2002) and the UK (ICO 2009). Scriven (2007) describes the usefulness of checklists in detail, and stresses how they are "easier for the lay stakeholder to understand and validate", reduce the "influence of the halo effect, i.e. the tendency to allow the presence of some highly valued feature to over influence one's judgment of merit" and economically incorporate "huge amounts of specific knowledge".

The PIA evaluation criteria are, therefore, first presented as a checklist (see Table 2), which is based upon several key sources, including the work of the PIAF project (Wright et al. 2011), as well as published research on the state of the art (Wright 2012) and on best practices (Wright and Paul 2012b) in privacy impact assessments.

The checklist avoids the problem of "dumbing down" the PIA process by providing a column on "scope for improvement" – it is more than a "mere box-ticking" exercise (Wright 2011).

Once our criteria are recognized, we apply weighting in line with the relative importance of each criterion. The weighting in Table 3 illustrates the high-level criteria (not the full detailed criteria in Table 2), and is based on the lessons learnt from the PIAF Report.

The criteria have been awarded weights in three categories – 1, 2 and 3, with 1 representing the least important and 3 representing the most important. The weighting is a subjective indication based on lessons learnt from the PIAF project.

We next determine the least important and the most important criteria. The basic criteria carry a weight of 1 (i.e. clarification of early initiation, identification of who conducted the PIA and publication). These criteria are in the nature of contextual details of the PIA process. While it is good practice to provide these elements, their absence is not such as to make the PIA a failure or useless. While these details are important, their absence can typically be addressed by contacting the PIA

Table 2. PIA evaluation checklist

PIA evaluation criteria	Yes	No	Scope for improvement
Early initiation	Tick where applicable		
Was the PIA initiated early enough to influence project design?			
Does the PIA report state whether the PIA was initiated early?			
Does the PIA report outline how the PIA influenced project design?			
Conduct of PIA			
Does the PIA report identify who conducted the PIA and their expertise/experience in PIA conduct?			
Does the PIA report identify when the PIA was conducted?			
Does the PIA report identify its target audience (i.e. for whom it was prepared)?			
Does the PIA report provide contact details for further information in relation to the PIA?			
Does the PIA outline/document the PIA process?			
Does the PIA report outline what guidance it followed?			
Does the PIA report state who approves it?			
Does the PIA outline a post-implementation review/audit process?			
Project description, purpose and relevant contextual information			
Does the report sufficiently describe the project being assessed and provide relevant contextual information (such as business rationale, project scope, or relevant social, economic or technological considerations)?			
Does the report describe the purpose and objectives of the project?			
Information flow mapping			
Does the PIA map the information flows? (i.e. how information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained)			
Legislative compliance checks			
Has all law relevant to the project been surveyed and the project checked for compliance?			
Identification of privacy risks and impacts[a]			
Does the PIA assess risks to data privacy?			
Does the PIA assess and indicate the level of risks to privacy of the person?			
Does the PIA assess and indicate the level of risks to personal behavior?			
Does the PIA assess and indicate the level of risks to personal communications?			

Table 2 (*Continued*)

PIA evaluation criteria	Yes	No	Scope for improvement
Does the PIA caution project managers and assessors that the risks listed in the PIA guide are not exhaustive?			
Does the PIA report make provisions to address issues arising out of future changes to the project?			
Does the PIA analyze the public acceptability of the scheme and its applications?			
Identification of solutions/options for risk avoidance, mitigation			
Does the PIA identify means/solutions for risk avoidance?			
Does the PIA identify means/solutions for risk mitigation?			
Recommendations			
Does the PIA make recommendations?			
Are the recommendations accompanied by timeframes for implementation?			
Have the recommendations been implemented/ incorporated in project design?			
Publication			
Has the PIA report/executive summary/edited version been published?			
If the PIA report is not published, has an explanation to that effect been made public?			
Identification of stakeholder consultation			
Have stakeholders been consulted as part of the PIA procss? Was the consultation adequate (representative of relevant interests)?			
Did stakeholders have the chance to provide information and comment?			
Does the PIA report document the stakeholder involvement and engagement process?			
Does the PIA incorporate stakeholder engagement throughout the project life cycle?			

Note: the term project may refer to a project, product, service, program or other initiative, including legislation and policy.

[a] The present article deliberately does not define and limit here what comes within the scope of the terms data privacy, privacy of the person, personal behavior or personal communications. We suggest the organizations refer to appropriate national PIA guidance for this information.

sponsoring organization; however, in some cases, their absence is an early warning in identifying other flaws in the process or the outcomes.

As one can see in Table 3, criteria that are important, carrying a weight of 2 (i.e. project description, information flow mapping, legislative compliance checks and identification of stakeholder consultation), are process-focussed. The elements these criteria look at must be included in the PIA report; their absence would make the PIA report ineffective and deficient, as they are a reflection of the thoroughness of the PIA process. These elements reflect how deeply the PIA process investigated the system, how

Table 3. Evaluation criteria and weights.

Evaluation criteria	Criteria weight
Clarification of early initiation	1
Identification of who conducted PIA	1
Project description, purpose and relevant contextual information	2
Information flow mapping	2
Legislative compliance checks	2
Identification of privacy risks and impacts	3
Identification of solutions/options for risk avoidance, mitigation	3
Recommendations	3
Publication	1
Identification of stakeholder consultation	2
Score	20

thoroughly it applied evaluation criteria, and how well it engaged stakeholders in the process.

Finally, the essential criteria carry a weight of 3 (i.e. identification of privacy risks and impacts, identification of solutions for avoidance, mitigation of privacy risks and recommendations). A PIA report that fails to incorporate these elements would be a failure, as these are the intended core outcomes of the PIA process itself.

To help determine whether the criteria are met or not and make an initial evaluation, we outline a detailed, descriptive checklist[5] with questions to help gage whether the criterion is fulfilled. The checklist was based on the best elements of PIA policy and practice identified in the PIAF Report and as outlined by Wright in his paper on the state of the art in PIA (Wright 2012).

The next task was to assign values – here too, we use a three-point scale with 2 indicating non-compliance, 5 part compliance and 8 indicating an effective level of compliance. In this respect, PEGS follows the AICPA/CICA scoring model.

Grades were assigned based on the following scores. Scores in the range of 141–160 are indicative of an excellent or effective PIA and graded as A+. Scores in the range of 121–140 are indicative of a very good PIA and graded as A −. Scores in the range of 101–120 are good and graded as B+. Scores between 81–100 are acceptable and graded as B −. Scores in the range of 61–80 are indicative of inadequate PIAs and are graded as C. Scores between 40 and 60 are indicative of poor PIAs and graded as D.

An excellent PIA is one that fulfills all the criteria to an exceptionally high degree. One must note, however, that there is no such thing as a perfect PIA, and yet efforts must be made to achieve that ideal. A very good PIA is one that is of high quality and yet not effective enough to meet the A+ standard. A good PIA is one that fulfills the necessary criteria and can be seen to be effective in most parts. It might be lacking in minor details. An acceptable PIA is one that fulfills the major requirements, yet leaves much to be desired. An inadequate PIA is one in need of major revision, and a failure refers to a PIA that fails to meet all or a substantial number of criteria.

The PEGS system and process

How does PEGS work in practice? Like some privacy risk assessment tools, PEGS could be embedded in a spreadsheet. PEGS could also be implemented as a web-based application.

There are two basic steps in the PEGS process. The first involves completing the checklist and the second involves the scoring and grade allocation.

Test driving PEGS

We now examine how PEGS could work in practice with the help of two case studies.

Case study 1 – the New Zealand Google street view PIA

As a first step, we analyze the New Zealand Google Street View PIA against the established evaluation criteria. Google Street View is a Google Maps application used to explore places through 360°, street-level imagery from public spaces and privately owned properties (that have permitted such access; Google Inc 2012). Google collects this imagery from its vehicles driving past locations, processes it and subsequently puts it online. Google Street View launched in New Zealand in 2008.

During the course of filming in New Zealand, Google's Street View vehicles collected open Wi-Fi information[6] (easily accessible Wi-Fi information such as network names) and payload information (the actual contents of communications) from unsecured Wi-Fi networks. When the revelation surfaced (New Zealand Privacy Commissioner 2010a), investigations followed. The Privacy Commissioner conducted an inquiry (New Zealand Privacy Commissioner 2010b), and eventually imposed several requirements on Google. One of the key requirements was to conduct a PIA on "new Street View data collection activities in New Zealand", and provide a copy of the PIA to the Privacy Commissioner.[7]

Google Inc. published an 11-page PIA report on its website (Google Inc 2011). We now examine it against the PEGS evaluation criteria.

The Google Street View PIA report does not satisfy the first criterion. The PIA was not initiated early enough to influence project design. The PIA is an example of a retrofit and was initiated as the result of obligation imposed upon Google by the New Zealand Privacy Commissioner after an inquiry into Street View's unauthorized collection of Wi-Fi information.

In relation to the second criterion (identification of who conducted the PIA), the Google Street View PIA report does not identify who conducted the PIA or name the author(s) of the PIA report.

Next, we checked compliance of the Street View PIA report to the third criterion – project description, purpose and relevant contextual information. The PIA report sets out a project description (overall aims, scope, extent and links of Street View to other projects). However, this is rather too brief (the project description minus the section on links to other projects is only a page long). Therefore, we find in favor of a part compliance score.

The Google Street View PIA partly fulfilled the fourth criterion, information flow mapping. Although information flows were mapped, their description left much to be desired (the New Zealand PIA Handbook recommends that flow charts clearly depict the manner of data collection, internal circulation and dissemination beyond the organization; Office of the Privacy Commissioner 2007).

Next, we analyzed compliance with the fifth criterion, legislative compliance checking. The PIA report mentions a "comprehensive legal assessment" (Google Inc 2011). However, the report does not explain how Google Street View complies specifically with relevant legislation, particularly the Information Privacy Principles of the Privacy Act 1993. The Report states that Google transfers Street View data outside New Zealand, yet does not (as the NZ PIA Handbook recommends) recognize any special sensitivities in this respect.

The Google Street View PIA Report highlights the privacy risks and impacts as necessitated by the sixth criterion (identification of privacy risks and impacts) and thus received a positive grading. The report covers the following privacy risks: generation of images incidentally featuring passers-by and information such as vehicle license plates; images triggering privacy-related sensitivities based on person–place association and images featuring sensitive locales (e.g. women's refuges; Google Inc 2011). However, when evaluated against the detailed checklist, it failed to demonstrate effective risk assessment; that is, there was no indication of risk levels, just an overall broad picture. The PIA report does not caution that the risks listed in the PIA are not exhaustive, or analyze the public acceptability of the scheme and its applications (this was particularly relevant given that Street View practices were found to be violating data protection law). Therefore, the report receives a part compliance score for this criterion.

The Google Street View PIA report fares well in relation to the seventh criterion – identification of solutions/options for risk avoidance, mitigation. The report outlines the measures taken to address privacy concerns prior to publication of images on Google Maps and Google Earth, for example, training of Street View vehicle operators prior to and during collection of imagery as well as guidance on appropriate route planning; disclosure to the public of collection activities (transparency about Street View's collection activities); outreach and education to sensitive groups regarding the launch and flagging process (which refers to the process whereby Street View users flag inappropriate content or sensitive imagery for Google to review and remove), delayed publication of images and automatic blurring of faces and license plates prior to the posting of imagery; and making available the "Report a Problem" tool (which enables members of the public to report a problem such as privacy concerns that they might have with the images Google captures). The tool is available as a link at the bottom left of a Street View image.

The Google Street View PIA report fulfills the eighth criterion in part – it includes recommendations in the PIA report (Google Inc 2011), but it does not provide any timeframes for implementation/incorporation in project design.

The Google Street View PIA report also fulfills the publication criterion. It is one of the few private company-based PIA reports in the public domain. It thus sets a good example for other companies in this respect.

In relation to the tenth criterion, stakeholder consultation, the Google Street View PIA report makes no mention of consultation whatsoever, especially of those stakeholders most affected by the implementation of Street View's collection and use of their personal information.

Case study 2 – the Australian EVI PIA

Our second case study concerns the Australian PIA on the proposal to amend the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) to authorize the use and disclosure of credit reporting information for electronic identity verification (EV; hereinafter the Australian EVI PIA; IIS 2009).

The Australian EVI PIA states that the PIA was initiated early enough to enable it to influence the proposal (ALRC 2008). Thus, it fulfills the first criterion. The

Australian EVI PIA report also identifies who conducted the PIA; that is, it was conducted by Information Integrity Solutions Pty Ltd for the Attorney-General's Department.

The Australian EVI PIA report adequately describes the proposal and its purpose, and provides relevant contextual information as required by the third criterion. It also complies with the information flow-mapping criterion. It contains a tabular analysis of the potential information flows (collection, use, disclosure, retention) if the use of credit information (CRI) for EV is authorized.

In relation to legislative compliance checks, the next criterion, the Australian EVI PIA report provides an overview of credit reporting and applicable regulations and how it would comply with those. Thus, it can be said to fulfill this criterion.

The next criterion is identification of privacy risks and impacts. This is the most detailed part of the Australian EVI PIA Report. The report identifies various privacy risks if identity information held by credit reporting databases were made available for electronic identity verification under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. It also considers the consequences of rejection/failure including black lists or other EV harms and the impact on individual control over their personal information.

An effective PIA should identify solutions and options for risk avoidance and/ or mitigation. The Australian EVI PIA Report contains recommendations (based on a "layered defence approach") categorized into two parts – recommendations relating to the law and recommendations relating to governance (including transparency and accountability). Thus, it scores well on both these criteria. A full score is awarded on the publication criterion, as the Australian EVI PIA report is publicly available.

It is only in relation to stakeholder consultation that the report falls short, according to our criteria. Although key stakeholders including privacy and consumer advocates, reporting entities and their representatives, CRAs and other EV service providers were consulted, the consultation seems to have been rather limited, given the scope of the proposal. Only 10 stakeholders were consulted, and only 10 submitted comments on the draft PIA report. Therefore, a part fulfillment of the last criterion is adduced.

Comparative analysis of the case studies. Based on the above analysis, we derive the results in Table 4, shown as a scorecard.

The New Zealand Google Street View PIA receives a score of 94, which makes it an acceptable PIA. The Australian EVI PIA on the other hand, scores very well and receives an A+ grade.

Role, functions and utility. PEGS is useful for a number of reasons.

First, evaluating a PIA will help increase transparency in PIAs. Second, it will help improve the quality of the PIAs. The PIAF Report recommended that PIA reports be quality assured by senior management (Wright et al. 2011). The PIA grading tool could facilitate this task. Third, it will increase accountability, particularly in the implementation of PIA recommendations. PEGS thus presents a viable, accessible and simple means of evaluating the rigor of an organization's PIA process.

Like the Privacy and Data Protection Impact Assessment Framework for RFID Applications, PEGS is sufficiently general in its approach – this means that it is dynamic enough for application across technologies and sectors.

PEGS could be used at different levels: by organizations to self-evaluate PIAs and meet and exceed legal requirements; by national data protection authorities to review

Table 4. Comparative chart with results of PIA report evaluation under PEGS.

Evaluation criteria for PIA reports	Criteria weight	Google streetview [NZ] compliance	Google streetview [NZ] Score	EVI [AU] compliance	EVI [AU] score
Clarification of early initiation	1	2	2	8	8
Identification of who conducted PIA	1	2	2	8	8
Project description, purpose and relevant contextual information	2	5	10	8	16
Information flow mapping	2	5	10	8	16
Legislative compliance checks	2	2	4	8	16
Identification of privacy risks and impacts	3	5	15	8	24
Identification of solutions/options for risk avoidance, mitigation	3	8	24	8	24
Recommendations	3	5	15	8	24
Publication	1	8	8	8	8
Identification of stakeholder consultation	2	2	4	5	10
Score	20	44	94	77	154
Grade		B −		A +	
Grade chart			Score assignment		
Excellent	A +	141–160	Complies fully		8
Very good	A −	121–140	Complies in part		5
Good	B +	101–120	Does not comply		2
Acceptable	B −	81–100			
Inadequate/requires improvement	C	61–80			
Failure	D	40–60			

PIAs conducted by organizations; and by third-party certification bodies and other stakeholders who need a user friendly means of determining in an objective manner whether a PIA is effective. Companies can use the PIA checklist/grading system as a self-evaluation mechanism to determine if their PIAs have been effective, or need to be improved and revised. It may even serve as a check on whether an organization is meeting its PIA commitments and as a reminder to the organization of its privacy commitments.

National data protection authorities or privacy commissioners can use the checklist/grading system to review and monitor PIA conduct and implementation. They can then provide feedback to the organizations in relation to the elements of the criteria found lacking. When data protection breaches occur, PEGS could be used to evaluate whether an organization had satisfied the requirements of PIA best practice, as outlined in the evaluation criteria. As such, the results of PEGS could become evidence of an organization's having exercised due diligence in relation to its PIA process.

PEGS is also useful to third party certification bodies. PEGS is based on international PIA best practice and presents a good model for third-party certification bodies to assess PIAs and determine privacy and data protection adequacy. Other stakeholders such as academics and the public could use either the checklist or the grading system to assess the quality of an organization's PIA. There is little to no guidance on how a layperson might assess a PIA. PEGS could fill that lacuna.

At this stage, we must also note the limitations of PEGS. Despite its intent to be as objective as possible, it is likely that some subjectivity owing to evaluator perceptions might creep into a PEGS analysis. Using two or more independent persons/parties to conduct the PEGS evaluation could address this.

Conclusion

This paper presents a model for PIA evaluation and grading that will enhance the effectiveness of PIAs. In this, it advances the state of the art in PIAs. However, to work effectively and to enhance the social value of PIAs, PEGS must be visible to stakeholders. This could be actualized by a central PIA registry[8] (or an online PIA portal like www.AllRovi.com) that uses PEGS to score and grade PIAs. This can be a "window of access" to PIAs and essential to build a PIA culture where organizations at different levels can learn from each other's experience and improve PIAs (Wright et al. 2011). This is all the more relevant given the policy thrust towards making PIAs more publicly accessible.

If the PEGS model is adopted, it will deliver further structure and standardization to the PIA process. The PEGS will be a means of informing and communicating with stakeholders about PIAs and their relative effectiveness. It will facilitate a judgment on a PIA's efficiency potential (i.e. how good a PIA is and to what it should aspire, and how future PIAs could be enhanced). One of the main reasons that companies conduct PIAs is to build trust – the PEGS results may be used to promote and advertise the achievement of that goal.

Acknowledgments

The authors prepared this paper on behalf of Trilateral Research & Consulting LLP based on research undertaken in the Privacy Impact Assessment Framework for Data Protection and

Privacy Rights (PIAF) project, funded by the European Commission's Directorate-General Justice under grant agreement number JUST/2010/FRAC/AG/1137-30-CE-0377117/00-70.

Notes

1. SIAs aim at ensuring that developments or planned interventions maximize the benefits and minimize the costs of those developments, including, especially, costs borne by the community.
2. The project began in January 2011 and its final deliverable was published in December 2012. Its objective was "encourage the EC and Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to the processing of personal data"; PIAF. http://piafproject.eu/
3. Generally Accepted Privacy Principles is a comprehensive privacy framework, developed under a joint effort of the CICA and the AICPA, designed to assist organizations create effective privacy programs addressing privacy risks and business opportunities. Available from: http://www.cica.ca/service-and-products/privacy/gen-accepted-privacy-principles/index.aspx
4. The tool's scope extends to RFID tags and readers as well as all connected backend systems and the communication infrastructure.
5. The checklist is not only useful post-PIA. It can serve as an effective aide memoir in preparing for a PIA, during the conduct of a PIA, preparing a PIA report or reviewing a draft version. The checklist is to be read in conjunction with PIA Guidance. This will help eliminate the "tunnel vision" problem associated with checklists. See Bisset (2001).
6. According to the New Zealand Privacy Commissioner, open Wi-Fi information includes the device's unique identity number, a user's network name, information on whether the network is secured or unsecured and signal strength.
7. Other requirements include making a statement about its Street View Wi-Fi collection activities on its official New Zealand blog (including an apology and acknowledgment of better transparency), improving privacy and information security training for all of its employees, improving review processes for its products and services and deleting payload data. These undertakings are in force for three years from 14 December 2010.
8. An example is the OIPC (2013).

References

AICPA/CICA. 2010. *AICPA/CICA Privacy Risk Assessment Tool User Guide.* 4. http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/privacyservices/downloadabledocuments/10684-378_privacy%20risk%20assessment%20tool.pdf

ALRC (Australian Law Reform Commission) 2008. *For Your Information: Australian Privacy Law and Practice. ALRC Report 108. Recommendation 57–4.* Accessed on November 21, 2012. http://www.alrc.gov.au/publications/57.%20Use%20and%20Disclosure%20of%20Credit%20Reporting%20Information/use-and-disclosure

Bisset, R. 2001. "Developments in EIA Methods." In *Environmental Impact Assessment: Theory and Practice*, edited by P Wathern, 47–61. London: Routledge.

European Commission. 2011. *Privacy and Data Protection Impact Assessment Framework for Radio Frequency Identification (RFID) Applications of 12 January 2011.* http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

European Parliament. 2011. *Resolution on a Comprehensive Approach on Personal Data Protection in the European Union, 2011/2025(INI).* Strasbourg: European Parliament.

European Parliament and the Council. 1995. "Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data." *Official Journal* L281: 31–50.

Flaherty, David H. 2000. *Privacy Impact Assessments: An Essential Tool for Data Protection. A Presentation to a Plenary Session on New Technologies, Security and Freedom. 22nd Annual Meeting of Privacy and Data Protection Officials.* Venice. 27–30. http://aspe.hhs.gov/datacncl/flaherty.htm

Google Inc. 2011. *Google Street View New Zealand Privacy Impact Assessment*. Accessed November 21, 2012. http://google-au.blogspot.in/2011/05/privacy-impact-assessment-for-street.html

Google Inc. 2012. *Using Street View*. Accessed November 21, 2012. http://maps.google.co.nz/intl/en/help/maps/streetview/learn/using-street-view.html

GS1 (2012). GS1 EPC/RFID. *Privacy Impact Assessment Tool*, http://www.gs1.org/epcglobal/pia

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

ICO (Information Commissioner's Office) 2009. *Privacy Impact Assessment Handbook. Version 2.0*. Cheshire. http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

IIS (Information Integrity Solutions Pty Ltd) 2009. *Privacy Impact Assessment Report, Electronically Verifying Identity Under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 Using Credit Reporting Information. For the Attorney General's Department*. http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(8AB0BDE05570AAD0EF9C283AA8F533E3) ~Privacy+Impact+Assessment+Report+-+Electronically+verifying+identity+under+the+AML+CTF+Act+using+credit+reporting+information.pdf

Institute for Management Information Systems. 2012. *Intelligent PIA User Manual*. Vienna University. Accessed November 21, 2012. http://www.wu.ac.at/ec/research/user_manual.pdf

Kemm, John, Jayne Parry, and Stephen Palmer, eds. 2004. *Health impact assessment: Concepts, Theory, Techniques and Applications*. Oxford: OUP.

Marx, Gary T. 2012. "Foreword: Privacy is Not Quite Like the Weather." In *Privacy Impact Assessment*, edited by David Wright and Paul de Hert, v–xiv. Springer: Dordrecht.

Morgan, Richard K. 1999. *Environmental Impact Assessment: A Methodological Approach*. United Kingdom: Chapman and Hall.

New Zealand Privacy Commissioner. 2010a. *Google and Wi-Fi Information Collection*. http://privacy.org.nz/media-release-google-and-wi-fi-information-collection/

New Zealand Privacy Commissioner. 2010b. *Google's Collection of WiFi Information During Street View Filming. Executive Summary*. http://privacy.org.nz/google-s-collection-of-wifi-information-during-street-view-filming/

OCIPO (Office of the Chief Information and Privacy Officer). 2010. *Privacy Impact Assessment Guide for the Ontario Public Service*. Canada: Queen's Printer for Ontario.

Office of Management and Budget. 2003. *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. Washington, DC. http://www.whitehouse.gov/omb/memoranda/m03-22.html

Office of the Privacy Commissioner. 2006. *Privacy Impact Assessment Guide*. Sydney, NSW. http://www.privacy.gov.au.

Office of the Privacy Commissioner. 2007. *Privacy Impact Assessment Handbook*. Auckland: Office of the Privacy Commissioner.

Office of the Privacy Commissioner. 2010. *Privacy Impact Assessment Guide*. Sydney, NSW. http://www.oaic.gov.au/publications/guidelines.html#privacy_guidelines

OIPC (Office of the Information and Privacy Commissioner of Alberta). 2013. *PIA Registry*. http://www.oipc.ab.ca/pages/PIAs/Registry.aspx

Radaelli, Claudio, and Fabrizio de Francesco. 2010. "Regulatory Impact Assessment." In *The Oxford Handbook of Regulation*, edited by R. Baldwin, M. Cave and M. Lodge, 279–301. Oxford: OUP.

Scriven, Michael. 2007. *The Logic and Methodology of Checklists*. http://www.wmich.edu/evalctr/archive_checklists/papers/logic&methodology_dec07.pdf.

Tancock, David, Siani Pearson, and, Andrew Charlesworth. 2010. "A Privacy Impact Assessment Tool for Cloud Computing." *Second IEEE International Conference on Cloud Computing*. Indiana University: USA, 667–676.

Treasury Board of Canada Secretariat. 2002. *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*. Ottawa. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp.

University of Pennsylvania. 2007. *Introduction to the SPIA Program*. http://www.upenn.edu/computing/security/spia/spia_step_by_step.pdf

Wright, David. 2011. "Should Privacy Impact Assessments be Mandatory?" *Communications of the ACM* 54 (8). http://cacm.acm.org/magazines/2011/8. doi:10.1145/1978542.1978568

Wright, David. 2012. “The State of the Art in Privacy Impact Assessment.” *Computer Law & Security Review* 28 (1): 54–61. doi:10.1016/j.clsr.2011.11.007.

Wright, David, and Paul De Hert. 2012a. “Introduction to Privacy Impact Assessment.” In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 3–32. Springer: Dordrecht.

Wright, David, and Paul De Hert. 2012b. “Findings and Recommendations.” In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 445–481. Dordrecht: Springer.

Wright, David, Kush Wadhwa, Paul De Hert, and Dariusz Kloza, eds, 21 September 2011. *PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights*, Deliverable D1, Prepared for the European Commission Directorate General Justice, JLS/ 2009-2010/DAP/AG. First deliverable (D1) prepared for the European Commission’s Directorate-General Justice under Grant Agreement Number JUST/2010/FRAC/AG/ 1137- 30-CE-0377117/00-70.