Should privacy impact assessments be mandatory?

By David Wright

Published in Communications of the ACM, Vol. 54, No. 8, August 2011.
http://cacm.acm.org/magazines/2011/8

Privacy impact assessment should be integrated into the overall approach to risk management with other strategic planning instruments.

This article considers the issue of whether privacy impact assessments (PIAs) should be mandatory. I will examine the benefits and disadvantages of PIAs, the case for and against mandatory PIAs, and ultimately conclude that they should be mandatory. Even if they are made mandatory, however, other factors, such as independent audits, need to be taken into account to make them truly effective.

CONTACTPOINT: SOLVING ONE PROBLEM AND CREATING ANOTHER

In the year 2000, an eight-year-old girl, Victoria Climbié, died from the unspeakable abuse she had suffered over many months at the hands of her great-aunt and the latter’s boyfriend. There was a huge public outcry as details of her case became known. The UK government eventually launched a public inquiry

The report of the public inquiry, led by Lord Laming and published in January 2003, found that Victoria’s murder could have been prevented had there been better communication between social services and other professionals who had visited her home [5].

The report led to the creation of a database, called ContactPoint, which the government said would improve child protection by improving the way information about children is shared among different social services so that tragedies like that of Victoria Climbié could be avoided in future.1 Launched in January 2009, the database was expected to hold information on about 11 million children in England.

While it might have been designed to solve one set of problems, the ContactPoint database created another set of problems: It attracted significant criticism over the risks to privacy and personal data protection [17]. The fact that some 330,000 people would have access to the database suggested that fears about the risks were not misplaced.2 There are a wide range of such risks – from identity theft to spamming to unauthorised, secondary use of personal data for research, for “sharing” with law enforcement agencies or other government agencies.

---

1 In fact, the idea of a child database preceded the Laming Report. It was suggested in a Cabinet Office report a year before. In his Foreword to the report, entitled Privacy and Data Sharing [23], then Prime Minister Tony Blair wrote, “The report concludes that there is great potential to make better use of personal information to deliver benefits to individuals and to society, including through increased data-sharing. But these benefits will only be realised if people trust the way that public services handle their personal data.”

2 A 2008 Eurobarometer report on citizens’ perceptions of data protection in the EU said that 64 per cent of respondents were concerned about the broad issue of the protection of privacy, a figure that has changed only slightly in previous polls since the early 1990s [6].
Should privacy impact assessments be mandatory?

benefit entitlement, for sale to insurance companies or companies engaged in personalised advertising.³

Former Information Commissioner Richard Thomas asked, “Is the collection of personal information about every child in the ContactPoint children’s database a proportionate way of balancing the opportunities to prevent harm and promote welfare against the implications for family privacy and the risks of misuse?”⁴ He answered his own question by saying that “One mechanism that could enable better decision-making is to conduct a privacy impact assessment to make clear the thinking behind a proposed data-sharing scheme and to demonstrate how the questions of proportionality are being addressed.”

ContactPoint is just one of many massive databases that governments and industry have created and continue to create and that would benefit from a privacy impact assessment at the design stage and perhaps at later stages too as an iterative process. In the instance of ContactPoint, the UK’s new coalition scrapped the database in August 2010 (it also scrapped the previous government’s plans for a national ID scheme).

WHAT IS A PRIVACY IMPACT ASSESSMENT?

Privacy impact assessments (PIAs) have been defined in various ways, but essentially a PIA is “a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme” and finding ways to mitigate or avoid any adverse effects.⁴ According to privacy expert Roger Clarke,

The concept of a PIA emerged and matured during the period 1995–2005. The driving force underlying its emergence is capable of two alternative interpretations. Firstly, demand for PIAs can be seen as a belated public reaction against the increasingly privacy-invasive actions of governments and corporations during the second half of the twentieth century. Increasing numbers of people want to know about organizations’ activities, and want to exercise control over their excesses… Alternatively, the adoption of PIAs can be seen as a natural development of rational management techniques… Significant numbers of governmental and corporate schemes have suffered low adoption and poor compliance, and been subjected to harmful attacks by the media. Organizations have accordingly come to appreciate that privacy is now a strategic variable. They have therefore factored it into their risk assessment and risk-management frameworks [4].

Clarke has identified various antecedents of privacy impact assessments – “It would… appear that the concept, although not yet the term, was in use in some quarters as early as the first half of the 1970s” – but the first use of the term or, at least, something very like it appears to be in a 1984 document of the Canadian Justice Committee which “recommended the submission of a privacy impact statement [by an agency to the Canadian Privacy Commissioner] in relevant situations.”⁵

³ These and many other privacy risks are apparent almost daily in our newspapers (a search on “privacy” in The New York Times brings up hundreds of examples). Examples can also be found in the References [1], [5], [10], [13], [18], [19] and [20]. Many privacy risks have been well known for a long time. See, for example, Westin’s classic Privacy and Freedom [25], published in 1967. Others make use of new technologies. See, for example, Robert O’Harrow’s No Place to Hide [16], published more recently (2005).
⁴ This definition combines two: one from the Treasury Board Secretariat of Canada [21], and one from Clarke [4]. Clarke has also compiled a list of various definitions in Appendix 1 of his paper.
⁵ The quote from the 1984 document was in Flaherty, David, Protecting privacy in surveillance societies, University of North Carolina Press, 1989, pp. 277–8, and cited by Clarke [4].
As PIAs are used in several different countries, it’s not surprising that there are some differences in the process – when they are triggered, who conducts the process, the reporting requirements, the scope, the involvement of stakeholders, accountability and transparency.

PIAs can also be distinguished from compliance checks, privacy audits and “prior checking”. A compliance check is to ensure a project complies with relevant legislation or regulation. A privacy audit is a detailed analysis of a project or system already in place which either confirms that the project meets the requisite privacy standards or highlights problems that need to be addressed [24].

Another important term to distinguish in this context is “prior checking”, which appears in Article 20 of the European Data Protection Directive and which says in part that “Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof” [9].

The European Data Protection Supervisor (EDPS) has a similar power under a Regulation of the European Parliament and Council, which obliges European Community institutions and bodies to inform the EDPS when they draw up administrative measures relating to the processing of personal data [8].

**WHO IS USING PIAS?**

Among the principal countries using privacy impact assessments are Australia, Canada, New Zealand, the UK and the United States. The European Commission also recommended use of privacy impact assessments in its Recommendation on RFID.6

In addition, the International Organization for Standardization (ISO) has produced a standard for PIAs in financial services [12], which describes the privacy impact assessment activity in general, defines the “common and required components” of a PIA, and provides guidance.

Although PIAs seem to be used most often by governments, some companies (e.g., Vodafone, Siemens and Nokia7) also apply privacy impact assessments, but there is little information available on which companies are using them, the extent to which they are used and whether their process is as thorough or as rigorous as the government institutions in the aforementioned countries.

While the approaches to privacy impact assessment are somewhat similar – i.e., the PIA process aims to identify impacts on privacy before a project is undertaken and measures to avoid or mitigate those risks – there are also important differences. This paper focuses on two, those of the UK and Canada. The author has chosen these two because the UK places emphasis on engaging stakeholders early in the PIA process and because Canada’s Office of the Privacy Commissioner has published detailed audits of PIAs. The most important

---

6 Article 4 says, “Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments” [7].

7 Representatives of these companies have contributed chapters to a book on privacy impact assessment co-edited by the author.
Should privacy impact assessments be mandatory?

difference between the two is that use of PIAs in the UK has been voluntary\textsuperscript{8}, while in Canada it is mandatory for federal government departments and institutions.

**UK**

In December 2007, the UK became the first country in Europe to publish a privacy impact assessment manual. The Information Commissioner’s Office published a second version in June 2009 [11].

Because organizations vary greatly in size and experience, and as the extent to which their activities might intrude on privacy also varies, the ICO says it is difficult to write a “one size fits all” guide. Instead, it envisages each organization undertaking a privacy impact assessment appropriate to its own circumstances.

The ICO says the privacy impact assessment process should begin as soon as possible, when the PIA can genuinely affect the development of a project. The ICO uses the term “project” throughout its handbook, but clarifies that it could equally refer to a system, database, program, application, service or a scheme, or an enhancement to any of these, or even draft legislation.

The ICO envisages a privacy impact assessment as a process that aims to:

- identify a project’s privacy impacts,
- understand and benefit from the perspectives of all stakeholders,
- understand the acceptability of the project and how people might be affected by it,
- identify and assess less privacy-invasive alternatives,
- identify ways of avoiding or mitigating negative impacts on privacy,
- document and publish the outcomes of the process.

The PIA process starts off with an initial assessment, which examines the project at an early stage, identifies stakeholders and makes an initial assessment of privacy risks. The ICO has appended some screening questions to its handbook the answers to which will help the organization decide whether a PIA is required, and if so, whether a full-scale or small-scale PIA is necessary.

A full-scale PIA has five phases:

In the **preliminary phase**, the organization proposing the project prepares a background paper for discussion with stakeholders, which describes the project’s objectives, scope and business rationale, the project’s design, an initial assessment of the potential privacy issues and risks, the options for dealing with them and a list of the stakeholders to be invited to contribute to the PIA.

---

\textsuperscript{8} There have been calls for mandatory PIAs in the UK too by, for example, the House of Lords in a June 2009 report [10, p. 73] and by former Information Commissioner Richard Thomas [10, p. 54; see also 19]. Interestingly, these calls have come after a Cabinet Office Data Handling Review stated that the government has accepted the value of PIAs and that they will be used in all departments [22, para 2.11]. An ICO representative said in a 10 Nov 2009 e-mail to the author that “The reason for Richard Thomas’ evidence appearing to contradict the Data Handling Review is that his evidence was given in 2007, before the Review was published. PIAs weren’t mandated by Cabinet Office at the time the evidence was given, but they were by the time the HoL [House of Lords] report was published. The Report went further than the Data Handling guidelines, in that it recommended amending the DPA [the Data Protection Act] to make PIAs a legal requirement. As far as I am aware there are no plans to put this recommendation into action.”
In the **preparation phase**, the organization should prepare a stakeholder analysis, develop a consultation plan and establish a PIA consultative group (PCG), comprising representatives of stakeholders.

The **consultation and analysis phase** involves consultations with stakeholders, risk analysis, identification of problems and the search for solutions. Effective consultation depends on all stakeholders being well-informed about the project, having the opportunity to convey their views and concerns, and developing confidence that their views are reflected in the outcomes of the PIA process.

The **documentation phase** documents the PIA process and outcomes in a PIA report, which should contain

- a description of the project,
- an analysis of the privacy issues arising from it,
- the business case justifying privacy intrusion and its implications,
- a discussion of alternatives considered and the rationale for the decisions made,
- a description of the design features adopted to reduce and avoid privacy intrusion and the implications of these features,
- an analysis of the public acceptability of the scheme and its applications.

The **review and audit phase** involves a review of how well the mitigation and avoidance measures were implemented.

Because projects vary greatly, the handbook provides guidance on the kinds of projects for which a small-scale PIA is appropriate. The phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalised and does not warrant as great an investment of time and resources in analysis and information-gathering. An important feature of the PIA as envisaged by ICO is that it should be transparent, accountable, include external consultation where appropriate, and make reports publicly available.

**Canada**

The Canadian government introduced its privacy impact assessment policy in May 2002 (which was superseded in July 2010 by a Directive on Privacy Impact Assessment). The policy specifically required that PIAs be conducted on all government initiatives that raise privacy risks and that the results of the analysis (along with the measures proposed to address the risks identified) be shared with the Office of the Privacy Commissioner (OPC) for review and comment. Government institutions have to post a summary of their PIAs on their websites [15].

Policy responsibility for the conduct of PIAs rests with a central agency, the Treasury Board Secretariat. Its PIA policy should be seen in the context of – or perhaps as a result of – surveys that show a majority of Canadians agree that the protection of personal information is one of the most important issues facing their country in the next 10 years [15, p. 6]. The policy puts the onus on institutions to demonstrate that their collection and use of personal information respects the Privacy Act of 1983 as well as the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000. It also obliges government institutions to communicate to citizens about why their personal information is being collected, how it will be used and disclosed, and how privacy impacts will be resolved.
Like the ICO, the Treasury Board Secretariat has prepared a handbook, a set of guidelines for undertaking PIAs. Like the ICO, the Privacy Commissioner of Canada views privacy impact assessment as a process. Also like the ICO PIA process, the Canadian guidelines are intended to increase the likelihood of anticipating, preventing and mitigating negative privacy consequences. Institutions are supposed to initiate the PIA in the early stages of the design of a program or service so that there is an opportunity to influence the program or service’s development. The PIA does not end after project design. It is intended to be an iterative process throughout the life cycle of the program or service.

Among the goals and outcomes of a PIA cited by the guidelines are these:
• Building trust and confidence with citizens;
• Promoting awareness and understanding of privacy issues;
• Ensuring that privacy protection is a key consideration in the initial framing of a project’s objectives and activities;
• Identifying accountability for privacy issues;
• Reducing the risks of having to terminate or substantially modify a program or service after its implementation in order to comply with privacy requirements;
• Providing decision-makers with the information necessary to make informed policy, system design, or procurement decisions based on an understanding of the privacy risks and the options available for mitigating those risks;
• Using anonymous information in lieu of personal information to achieve the same program objectives;
• Possibly deciding to abandon a project at an early stage based on the significance of the privacy risks;
• Promoting open communications, common understanding and transparency.

The guidelines have four main steps:

**Step 1: Project initiation** is to determine whether a PIA is required. The first question to ask is: “Is personal information being collected, used or disclosed in this initiative?” If the initiative is at the early concept or design stage and detailed information is unknown, then government departments and agencies can conduct a preliminary privacy impact assessment, which is not as comprehensive as a full PIA but will indicate whether a proposal has significant privacy risks.

**Step 2: Data flow analysis** is to examine how personal information will be collected, used, disclosed and retained.

**Step 3: Privacy analysis** consists of responses to a series of questions aimed at helping to identify the privacy risks or vulnerabilities associated with the proposal.

**Step 4: Privacy impact analysis report** is a documented evaluation of the privacy risks and the associated implications of those risks along with a discussion of possible remedies. The PIA report should convey the following information:
• A detailed description of the proposal including objectives, rationale, clients, approach, programs and/or partners involved,
• A list of all the data elements involving personal information,
• A list of all stakeholders, their roles and responsibilities,
Should privacy impact assessments be mandatory?

- A list of relevant legislation and policies,
- A description of the specific privacy risks,
- Possible options to eliminate or mitigate privacy risks,
- A description of any residual or outstanding risks,
- An outline of a privacy-oriented communications strategy.

Although the Canadian PIA has the virtue of being mandatory for government institutions, the guidelines are not clear on when and how stakeholders should be engaged or consulted, which is emphasised in ICO’s PIA handbook. Nor is it clear why only a summary of the PIA is to be posted on an institution’s website rather than the full PIA as is done in the US. Lists of questions feature in both the UK and Canadian PIA guidelines, and some might view such checklists, particularly those requiring mere yes/no responses, as “dumbing down” the PIA notion in a manner inconsistent with the real needs of risk assessment. On balance, the questions seem useful as they are likely to stimulate consideration of issues that might not otherwise occur to project managers. In any event, in both the UK and Canadian guidelines, project managers are obliged not to simply answer yes or no, but also to provide details in their responses to the questions.

**Benefits of PIAs**

Proponents have adduced various benefits from undertaking a PIA:

- Identifying and managing risks – Undertaking a PIA will help industry and government to avoid misjudging what the media and the public will accept in regard to impacts on privacy. With the growth in data-intensity and increasing use of privacy-intrusive technologies, the risks of a project or scheme being rejected by the public are increasing.
- Avoiding unnecessary costs – By performing a PIA early, an organization avoids problems being discovered at a later stage, when the costs of making significant changes or cancelling a flawed project outright are much greater.
- Avoiding inadequate solutions – Solutions devised at a later stage are often not as effective at managing privacy risks as solutions designed into the project from the start. “Bolt-on solutions devised only after a project is up and running can often be a sticking plaster on an open wound.”
- Avoiding loss of trust and reputation – A PIA will help an organization’s reputation and avoid deploying a system with privacy flaws which attract negative attention from the media, competitors, public interest advocacy groups, regulators and customers. Retrospective imposition of regulatory conditions may put the entire project at risk. A PIA provides an opportunity to obtain commitment from stakeholders early on and to avoid the emergence of opposition at a later, more costly stage.
- Understanding the perspectives of stakeholders – Inputs from stakeholders may lead to a better-designed project, the difference between a privacy-invasive and a privacy-enhancing project, and pre-empt possible misinformation campaigns by opponents.
- Providing a credible source of information to assuage alarmist fears and alerting the complacent to potential pitfalls.
- Imposing the burden of proof for the harmlessness of a new technology, process, service or product on its promoters.
- Achieving a better balance among conflicting interests.
- Improving public awareness and making available more information about an envisaged system, service or project.

9 The quote comes from Chapter 1 of the ICO PIA handbook [11].
• Improving security of personal data and making life more difficult for cyber criminals.\textsuperscript{10}

Two examples of the effectiveness of privacy impact assessments are the following. In both cases, unduly privacy-intrusive projects were abandoned.

In 2007, the US Department of Homeland Security (DHS) was developing a data mining tool known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) to help detect terrorism and other threats. The US Government Accountability Office (GAO) was asked to review the tool and potential privacy impacts that could arise from its use. The GAO said use of the ADVISE tool raised a number of privacy risks including the potential for erroneous association of individuals with crime or terrorism, the misidentification of individuals with similar names and a potentially costly retrofit at a later date. It said a privacy impact assessment would identify specific privacy risks and help officials determine what controls are needed to mitigate those risks. It noted that the E-Government Act emphasizes the need to assess privacy risks early in systems development and recommended that DHS should immediately conduct a privacy impact assessment of the tool. Following the GAO report and further reports by the DHS Privacy Office and Inspector General citing privacy concerns, DHS terminated the ADVISE tool.\textsuperscript{11}

The Intelligence Reform and Terrorism Prevention Act of 2004 requires the US government to collect biometric data from individuals visiting the US. DHS proposed use of passive RFID tags embedded in arrival/departure forms to track entry and exit of foreign visitors at border crossings. A GAO report issued in January 2007 noted that in addition to technical deficiencies with the proposed system, “the technology that had been tested cannot meet a key goal of US-VISIT—ensuring that visitors who enter the country are the same ones who leave.”\textsuperscript{12} DHS Secretary Michael Chertoff announced in February 2007 that DHS was abandoning the program. Experts believe the intense examination of the program’s objective, performance and risks that led to its abandonment was greatly facilitated by the PIA process and the ongoing examination and attention to the privacy and security issues posed by the program by the Data Privacy and Integrity Advisory Committee, Congress, and the public.

\textbf{DISADVANTAGES OF PIAS}

Opponents of PIAs could criticize them as adding to the bureaucracy of decision-making and as something that will lead to delays in implementing a project. They might say that conducting PIAs runs counter to the notion of streamlining government, of reducing red tape and regulatory burden. Proponents could respond that initiating a PIA at the earliest stages of project planning may actually lead to savings in time and costs downstream, i.e., if a project proceeds without a PIA, then there may be opposition to the project when the implications of the project become known and such opposition may lead to delays in its implementation or outright cancellation.

Undertaking a PIA is not cost free. While the costs will be largely borne by the government or company wishing to undertake a project or to provide a new service, other stakeholders wishing to participate in a PIA will incur costs too, e.g., in researching alternatives to

\textsuperscript{10} These benefits have been adapted from the ICO PIA Handbook [11] and from the New Zealand Privacy Impact Assessment Handbook [14].
\textsuperscript{11} http://www.gao.gov/products/GAO-07-293
\textsuperscript{12} This case has been examined in detail in Bamberger and Mulligan [1, p. 78].
Should privacy impact assessments be mandatory?

proposed implementation schemes and in making representations to the project manager and, if their concerns are not addressed, in stimulating negative publicity. They may also incur additional costs in monitoring the way in which the project is implemented or service provided after the PIA.

Opponents might also be against PIAs because PIAs might upset information asymmetries which are now in their favour. A PIA would require them not only to be more forthcoming in ensuring that all stakeholders have the same information at their fingertips, but also to make efforts towards achieving consensus with other stakeholders.

While some have characterized the private sector as having a reactionary, hostile approach towards PIAs [4], entrepreneurs, whether in government or industry, may now be adopting a view that PIAs are, after all, a form of risk assessment, and if a PIA can help reduce risk, then it is a tool not without merits.

SHOULD PIAS BE MANDATORY?

Although privacy experts and regulators see numerous benefits of PIAs\(^\text{13}\), such as those cited above, PIAs are not yet in wide use. That fact, together with the continuing and widespread risks to privacy and personal data protection, raises the question: should PIAs be mandatory?

PIAs are not mandatory in most jurisdictions. In May 2002, the Canadian government became the first jurisdiction to make PIAs mandatory for government institutions [3, p. 261], but it has not imposed a similar obligation on the private sector. In the UK, there is currently no formal Parliamentary backing for PIAs, and the ICO can only recommend their completion [24]. As noted above in footnote 8, the Cabinet Office has said that they will be used in all departments [22, p. 19]. However, there is no reporting mechanism in place whereby, for example, a government department is obliged to inform ICO of the PIA or the Treasury in making submissions for funding programs. PIAs are also mandatory for US government agencies under the E-Government Act of 2002\(^\text{14}\), and the European Commission is also considering make some PIAs mandatory as part of its revision of the EU Data Protection Directive which is to be published later this year.

What does a mandatory PIA mean?

In Canada’s case, it means government institutions are obliged to carry out privacy impact assessments and to include the results of their PIAs when they make submissions for funding to the Treasury Board Secretariat.

Government institutions are obliged

\(^{13}\) See, for example, Warren et al [24, p. 234], the NZ Privacy Commissioner [14, p. 11] and ICO [11, Ch. 1].

\(^{14}\) The US E-Government Act of 2002 obliges federal agencies to conduct PIAs before developing or procuring IT systems or projects that collect, maintain or disseminate personally identifiable information. The PIAs are to be reviewed by an agency’s Chief Information Officer, or equivalent official – someone other than the official procuring the system or who conducts the PIA – and posted on the agency’s website and/or published in the Federal Register. This requirement may be waived for security reasons or to protect classified or commercially sensitive information. The Office of Management and Budget (OMB) provides guidance on how PIAs are to be conducted. Agencies are supposed to conduct PIAs before making budgetary submissions to the OMB. There is no provision in either the E-Government Act or the OMB guidance for any external stakeholder consultation on draft PIAs. Nevertheless, PIAs are regarded as one of the more positive aspects of American privacy protection policy in the last 10 years [2, p. 11].
Should privacy impact assessments be mandatory?

- to conduct PIAs at the time of program or service design for all new initiatives (or substantially redesigned programs and services) that may raise privacy risks;
- to provide a copy of the final PIA, approved by the Deputy Head, to the Office of the Privacy Commissioner, prior to implementing the initiative, program or service;
- to develop risk assessment and mitigating measures for privacy issues identified and to ensure that privacy mitigating measures are implemented; and
- to make PIA summaries public.

They are expected to show evidence of:

- programs in place to inform staff and other stakeholders of the PIA policy’s objectives and requirements;
- formally defined program responsibilities and accountabilities;
- a system to 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 compliance monitoring; and
- adequate resources committed to support the department’s obligations under the PIA policy.

**THE CASE FOR MANDATORY PIAS**

There are various reasons why PIAs should be mandatory, but the two key arguments are that privacy risks are of epidemic proportions and they provoke such loss of confidence among consumer-citizens that they undermine e-government and e-commerce.

Data breaches and losses have afflicted both the public and private sectors. Some have involved the loss of millions of records. The most publicised case in the UK involved the loss in October 2007 of personal data records for 25 million individuals and 7.25 million families receiving child benefits by Her Majesty’s Revenue and Customs (HMRC) [18]. In the following 12 months, the number of reported breaches and losses of personal data “soared” [19]. More recent figures suggest that the number of breaches is getting even worse with seven in 10 UK organizations having experienced a data breach in the year to July 2009, up from 60 per cent in the previous year [13]. Other countries have had similar experiences.

Such breaches and losses lend weight to the idea that information systems should be “regarded as (relatively) dangerous until shown to be (relatively) safe, rather than the other way around” [3, p. 62]. In other words, the onus should be on those proposing new projects, systems or services that involve personal data to prove that the benefits outweigh the costs, that the risks can be avoided, contained or mitigated.

PIAs should be mandatory not only as a way of responding to breaches and losses, but as a way of responding to potentially privacy-intrusive projects and services.

PIAs would complement data protection legislation and help to increase awareness of the exigencies and obligations imposed by such legislation.

High levels of accountability and transparency are vital to the way organizations handle and share personal information, yet these are all too often absent [20, p. 2]. Mandatory PIAs would be an excellent way of ensuring accountability and transparency.
Should privacy impact assessments be mandatory?

**The case against mandatory PIAs**

Some might argue that there is no need for privacy impact assessments, let alone mandatory PIAs, so long as privacy and data protection legislation is properly respected and enforced. Unfortunately, that argument is undercut by the increasing intrusions upon privacy and the inadequate safeguards of personal data that characterise our social polity today.

An argument against mandatory PIAs is that it would require new legislation, especially if PIAs were to be mandatory for both government and industry. Arguably, such legislation could be quite complex as some discretion would be needed with regard to the scale and circumstances of the PIA.

Making PIAs mandatory would undoubtedly increase the resources, time and cost it takes to implement projects, at least in the short term, but, as mentioned above, such time and cost may be a good investment if they lead to avoidance or mitigation of risks and if they foster trust and confidence among citizen-consumers.

A further argument against mandatory PIAs is that, by imposing them as an element of bureaucracy, PIAs will “get a bad name” and be performed perfunctorily. Some people will treat PIAs as things they have to do, rather than things they should do to mitigate risk [2, p. 11]. An antidote to perfunctory PIAs is third-party reviews and audits as well as tying the PIAs to funding submissions, as is supposed to happen in both Canada and the US.

Some might argue against placing undue reliance on mandatory PIAs as the PIA process is only as good as the people involved. That is true. No matter how good the PIA guidance, organizations will need to invest in training staff, raising their awareness and commitment to an effective, transparent PIA with responsibility and accountability placed at the top of the organizational hierarchy.\(^{15}\)

PIAs are only valuable if they have, and are perceived to have, the potential to alter proposed initiatives in order to mitigate privacy risks. Where they are conducted in a mechanical fashion for the purposes of satisfying a legislative or bureaucratic requirement, they are often regarded as exercises in legitimisation rather than risk assessment [24].

**WILL PIAs BECOME A HUGE ADMINISTRATIVE BURDEN?**

PIAs have a cost and they require resources. The nature and extent of resources will vary depending on the scope and complexity of the proposed project. Having said that, when the organization has an established privacy strategy and experience in the process involved, it’s been estimated that a small-scale PIA could be completed quite quickly, in some instances, in a matter of hours [24].

Nevertheless, the Office of the Privacy Commissioner of Canada has admitted that conducting PIAs and implementing PIA policy is time and resource intensive. In fact, in its audit report, it said even more resources should be devoted to the process [15].

Although the Treasury Board Secretariat suggests a delivery standard of six weeks for the OPC to review the privacy impact assessments submitted to it, the OPC said that its own

---

\(^{15}\) The paper by Bamberger and Mulligan [1] shows how important is the role played by the chief privacy officer, the independence and reporting relationship accorded to the CPO and the individuals recruited for those roles.
Should privacy impact assessments be mandatory?

shortage of human resources meant that it was taking much longer, in many cases 18 months longer, to review a submission [15]. It said that generally resources for PIAs were “severely stretched” and that the full costs of conducting PIAs were generally not well defined.

The UK ICO handbook says that whether a full-scale or small-scale PIA should be carried out depends on the magnitude of the privacy risks. The Canadian PIA guidelines offer a somewhat similar approach.

In some cases, as with shared service or system initiatives where entities use the same or similar approaches to the collection, use and disclosure of personal information, generic assessments might be possible.

BEYOND MANDATORY PIAS – AUDITS AND METRICS

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.

The ICO does not keep statistics on the use of PIAs in the public or private sectors, nor does it require entities to notify it that they are carrying out a PIA, unlike its Canadian counterpart which does. In fact, the OPC has gone even further and suggested creation of a central database or registry of privacy impact assessments, which would provide a single window of access to PIAs and privacy intrusive projects across government. The registry would help the public to better understand the substance and privacy impacts of government projects and would help the Treasury Board Secretariat and the OPC to monitor PIA activities. The registry might also improve the project management capability of institutions and work to reduce or eliminate PIA omissions. It might also improve the transparency of government operations and help to better engage the public and Parliamentarians on privacy matters.

The most detailed published audits of privacy impact assessment practice are those carried out by OPC. In 2007, five years after the Canadian government introduced its policy on privacy impact assessments, the OPC carried out an audit in nine major government departments (including Health Canada) and institutions (including the RCMP) and conducted a survey of 47 others [15]. The audit identified a number of good practices and singled out those institutions performing them.

It also found varying degrees of commitment to the policy. Some government institutions had made serious efforts to apply the directive, and the policy was beginning to have the desired effect of promoting awareness and understanding of the privacy implications associated with program and service delivery. Nevertheless, it said that government institutions still had to make more effort in order to meet their commitments.

Among the problems found by the OPC were the following:

---

16 It gives advice to organizations that approach it, but it does not record the contact. PIAs have been designed to be a self-assessment tool, so while the ICO works to promote its use, it does not have “ownership” of the PIA process and leaves it for organizations to implement as they see appropriate. The ICO reckons it has been approached by hundreds of organizations re PIAs. Most of these have been public authorities. The process in the handbook is designed to be generic so these companies can adapt it for their own needs without having to consult the ICO. Thomas Oppe, ICO, in an 11 Aug 2009 e-mail to the author.
Of the 47 federal institutions polled, 89 per cent of respondents said they used personal information in the delivery of programs and services. Beyond having the necessary resource capacity to fully implement the policy, the single most important determinant in ensuring the success of privacy impact assessments was the existence of a sound management control framework. Two-thirds (68 per cent) said they did not have such a framework in place. The most common weakness identified within the management systems was the lack of a formal screening process to identify when a PIA should be undertaken.

Only a minority of government institutions were posting the results of PIA reports on their websites and most of those were of poor quality. Some PIA submissions continue to lack detailed action plans for the implementation of privacy protection strategies. It also found that institutions are generally slow in addressing the identified privacy risks. The audit found evidence that departments were not properly monitoring the implementation of risk-mitigating measures. The audit noted numerous cases where PIAs were not initiated until well after a project’s conception or design. Additional training and guidance were needed to make program managers aware of their responsibilities under the policy and to give them the privacy knowledge and skills necessary to conduct PIAs.

The PIA policy states that the implementation of the policy should be monitored, in part, through internal audits, but the OPC found that none of the institutions surveyed had conducted comprehensive audits for compliance with the PIA policy. The report said that the conduct of internal audits would complement and enhance institutional control activities and ensure that risks identified from the PIA process are sufficiently mitigated. It recommended that the internal audit branches of all federal institutions should seek to include privacy and PIA-related reviews in their plans and priorities.

The OPC opined that greater scrutiny generated by public exposure can prompt greater care in the preparation of PIAs and provide Parliament and the public with the necessary information to have more informed debates concerning privacy protection. Public disclosure may also provide additional assurance that privacy impacts are being appropriately considered in the development of programs, plans and policies – essentially holding each institution to account for the adequacy of its privacy analysis.

**CONCLUSIONS**

Many breaches in databases and losses of personal data held by government and industry have received a lot of negative publicity in the media. Undoubtedly, there are more breaches and losses that have not been reported by the media. Even so, those that have been reported take their toll in public trust and confidence. Most people simply do not believe their personal data is safe. There are justified fears that their personal data is used in ways not originally intended, fears of mission creep, of privacy intrusions, of our being in a surveillance society. Such fears and apprehensions slow down the development of e-government and e-commerce, and undermine trust in our public institutions.

As databases are established, grow and are shared, so do the risks to our data. A breach or loss of personal data should be regarded as a distinct risk for any organization, especially in view of surveys that show most organizations have experienced intrusions and losses. Assuming that most organizations want to minimize their risks, then privacy impact assessments should be seen as a specialized and powerful tool for risk management. Indeed, PIAs should be
Should privacy impact assessments be mandatory?

integrated into the overall approach to risk management and with other strategic planning instruments [15].

Even if PIAs seem like a logical tool to use by any organization dealing with personal data, many organizations are not likely to use the tool unless they are obliged to. Given the risks involved and taking into account the number and magnitude of breaches, intrusions and other privacy risks, the case for mandatory privacy impact assessments seems unassailable, for both the public and private sectors. Under a policy of mandatory PIA, organizations would be obliged to conduct a preliminary assessment and if the project might have privacy impacts, then it would be compulsory to perform a PIA, but one that reflects the nature and scale of the project and its potential privacy impacts – i.e., a PIA need not be disproportionately large, expensive or long. From the author’s perspective, the Canadian approach (see above) should be the baseline for mandatory PIAs, but “tweaked” a bit – e.g., it should be mandatory to consult with stakeholders early on (as in the UK) and to post full PIAs on the Web (redacted, if necessary, for security or commercially competitive reasons) as in the US. PIAs should also be subject to third-party audit.

But are mandatory PIAs enough?

Unfortunately, no. Clearly, the most effective way to protect personal information is to use a combination of tools and strategies which include complying with legislation and policy, using privacy-enhancing technologies and architectures and engaging in public education as well as conducting privacy impact assessments.

If some governments are reluctant to make PIAs mandatory for the private sector, governments could introduce some market incentives. For example, procurement policies and publicly funded research could build in a requirement for privacy impact assessments in their criteria for awarding contracts.

Mergers and acquisitions currently assessed only on competition grounds could also be assessed in terms of privacy impacts, which would improve transparency, help to minimize encroachments on privacy and identify any intended repurposing of data.

Any cross-jurisdictional agreements involving personal data could be subject to PIAs, and any service providers intending to offer a service subject to regulatory approval could be required to carry out a PIA.

As valuable as PIAs are as a risk management tool, they are typically concerned with assessing the privacy impacts of individual projects, programs or services. There remains a need to deal with the broader privacy implications of plans and policies that cut across a mix of policies or programs or services.

An important finding of the Canadian audit was that little consideration had been given to projects involving the intra-institutional, inter-institutional or cross-jurisdictional flow of personal information. Although the PIA policy states the need to conduct a PIA in situations where programs or services are contracted out or devolved to another organization, there is no clear requirement for doing so in cases of information sharing. As government programs and initiatives become increasingly integrated, and as data sharing activities within government
Should privacy impact assessments be mandatory?

become more commonplace, the risk of privacy breaches or improper personal information handling practices increases accordingly [15, p. 16].

The audit also expressed concerns about the long-term changes that may occur to an individual’s privacy, not only as a result of a single isolated action but by the combined effects of successive and interdependent intervention. The incremental effects on the integrity of personal information may be significant from a privacy point of view even when the effects of each successive action, independently assessed, are considered insignificant. Consequently, PIAs should consider the cumulative privacy effects that are likely to result from a program in combination with other projects or activities that have been or will be carried out.

Whether PIAs will gain enough traction to become mandatory for both government and industry remains to be seen. There are positive signs, however. Industry developed a PIA Framework for RFID which was approved by Europe’s data protection authorities, represented in the Article 29 Data Protection Working Party, in February 2011, which calls for PIA to be carried out for RFID applications. The European Commission has said it will examine the possibility of including in its new data protection framework, to be published later this year, “an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are 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”.

PIA proponents will be watching with interest.

ACKNOWLEDGEMENT

The author would like to thank the anonymous reviewers for their helpful and constructive suggestions for improving this article.

REFERENCES


Thomas and Walport raised a similar concern in their Data-Sharing Review Report [20, p. 44]. They said there was “far too little transparency” about the identification of bodies with whom organizations share personal information. Organizations should publish – and regularly update – a list of other organizations with which they share personal information.

Should privacy impact assessments be mandatory?


Should privacy impact assessments be mandatory?


David Wright (david.wright@trilateralresearch.com) is founder and managing partner of Trilateral Research and Consulting LLP, based in London, U.K. He is the co-editor of the book *Privacy Impact Assessment* to be published by Springer later this year.