The Information Society, 29: 307–315, 2013
Published with license by Taylor & Francis
ISSN: 0197-2243 print / 1087-6537 online
DOI: 10.1080/01972243.2013.825687

Routledge
Taylor & Francis Group

PERSPECTIVE

Making Privacy Impact Assessment More Effective

David Wright

Trilateral Research & Consulting, London, United Kingdom

Europe's proposed Data Protection Regulation is expected to make data protection impact assessment (DPIA) mandatory, a development that could impact hundreds of thousands of organizations (both governmental and private sector) in Europe, as well as non-European entities offering their wares and services there. This article reviews the DPIA provisions outlined in the new regulation. For the nuts and bolts of a privacy impact assessment (PIA) methodology, Europe could select features from the PIA methodologies used in Australia, Canada, Ireland, New Zealand, the United Kingdom, and the United States, the countries with the most experience in PIA. A European Commission (EC)-funded project, called PIAF, reviewed these various methodologies and proposed an "optimized" PIA for Europe (and elsewhere) based on the best practices of the aforementioned countries. Based on these best practices, this article outlines a 16-step PIA process. It argues that while some organizations may regard a PIA as a hassle, in fact, a PIA offers many benefits, as spotlighted in the article.

Keywords consultation, PIAF, privacy impact assessment, privacy risks, stakeholders

The European Commission (EC) officially released its package for reform of the data protection framework in Europe on January 25, 2012. The centerpiece of the reform package was the proposed Data Protection Regulation, Article 33 of which would make privacy impact assessment (PIA; the regulation uses the term "data protection impact assessment" [DPIA]) mandatory "where processing operations present specific risks to the rights and freedoms of data subjects [individuals]" (European Commission 2012, 62–63).

Received 4 December 2012; accepted 4 July 2013.
Address correspondence to David Wright, Trilateral Research & Consulting, Crown House, 72 Hammersmith Road, London, W14 8H, United Kingdom. E-mail: david.wright@trilateralresearch.com

Article 33 sets out examples of specific risks, including processing involving evaluation of a person's economic situation, location, health, personal preferences, reliability and behavior, sex life, health, race, and ethnic origin; video surveillance; genetic and biometric data; and other potentially problematic data-processing operations.

Article 33 briefly describes what a PIA report shall contain—"at least" a general description of the envisaged processing operations, an assessment of the risks to data subjects, the measures envisaged to address those risks, safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation. The proposed regulation would require data controllers to seek the views of data subjects or their representatives on the intended processing. This provision is interesting because several privacy commissioners advocate stakeholder consultation but, in practice, such consultation is infrequent at best. A mandatory PIA may change that.

The PIA requirements described in Article 33 are rather sketchy; hence, the commission includes a provision that would empower it to specify additional criteria and conditions at a later time, including conditions for "scalability, verification and auditability," and to define standards and procedures for carrying out, verifying, and auditing PIAs. Data protection authorities across Europe, as represented in the Article 29 Data Protection Working Party (Article 29 WP; the Working Party), have generally supported the provisions of Article 33. In its March 2012 opinion, the Working Party said it "welcomes the inclusion of provisions that give incentives to controllers to invest, from the start, in getting data protection right (such as data protection impact assessments, data protection by design and data protection by default). The proposals place clear responsibility and accountability on those processing personal data" (Article 29 WP 2012, 4).

While the Working Party welcomed the obligation to carry out a PIA, it had some specific suggestions for improvement of Article 33. For example, it suggested that

the limitation under Article 33 to processing "on a large scale" should be deleted, as the Working Party believes that a PIA should be "required for such processing operations even on a small scale" (Article 29 WP 2012, 16). Here, as elsewhere, the Article 29 WP is of the view that PIAs should be used even more widely than proposed by the commission.

Within the context of these developments, Europe has the opportunity to formulate a state-of-the-art PIA methodology in advance of the adoption of the new regulation. To advance that objective, this article outlines the key elements and structure of such a methodology.

DIFFERENT PIA METHODOLOGIES

Europe can learn from earlier experience in developing an effective PIA methodology, which is to say that several other countries have been using PIAs, in some instances for more than a decade. The countries with the most experience are Australia, Canada, Ireland, New Zealand, the United Kingdom, and the United States. The following paragraphs offer a thumbnail sketch of the principal PIA policies and methodologies.[1] While there are differences in the methodologies, all of them are concerned with identification of risks to privacy and ways of overcoming those risks. Elsewhere (Wright, Finn, and Rodrigues 2013), the author has made a comparative assessment of the various PIA policies and practices using a set of 18 criteria derived from the PIA literature, notably papers prepared by PIA pioneers such as Roger Clarke, Blair Stewart, David Flaherty, Nigel Waters, and Elizabeth Longworth. The 18 assessment criteria include the following:

1. Does the PIA guide provide a privacy threshold assessment to determine whether a PIA is necessary?
2. Does it advocate undertaking a PIA for proposed legislation and/or policy as well as projects?
3. Is PIA regarded as a process?
4. Does the PIA guide target both companies as well as governments?
5. Does the PIA address all types of privacy (informational, bodily, territorial, locational, communications)?
6. Is PIA regarded as a form of risk management?
7. Does the PIA guide identify privacy risks?
8. Does the PIA guide contain a set of questions to uncover privacy risks?
9. Does the PIA guide identify possible strategies for mitigating those risks?
10. Does the guide explicitly say that PIA is more than a compliance check?
11. Does the PIA guide identify benefits of undertaking a PIA?
12. Does the PIA guide support consultation with external stakeholders?
13. Does the PIA guide provide a suggested structure for the PIA report?
14. Does the guide say that PIAs should be reviewed and updated throughout the life of a project?
15. Does the PIA guide encourage publication of the PIA report?
16. Does the PIA policy provide for third-party, independent review or audit of the completed PIA report?
17. Is PIA mandated by law, government policy, or must a PIA accompany budget submissions?
18. Do PIA reports have to be signed off by senior management (to foster accountability)?

In Australia, the Office of the Privacy Commissioner (OPC, now the Office of the Australian Information Commissioner, OAIC) published its *Privacy Impact Assessment Guide* (the *Guide*) in August 2006, and a revised version in May 2010 (OPC 2010). The *Guide* is addressed to government agencies, the private sector, and the not-for-profit sector (i.e., civil society organizations). However, there is no legislative requirement in Australia to conduct a PIA. The *Guide* (OPC 2010, xii) does not impose a particular PIA style ("There is no one-size-fits-all PIA model") but suggests a flexible approach depending on the nature of the project and the information collected. The *Guide* says that "Consultation with key stakeholders is basic to the PIA process" (OPC 2010, x). The *Guide* encourages organizations, "where appropriate," to make the PIA findings available to the public.[2] Publication "adds value; demonstrates to stakeholders and the community that the project has undergone critical privacy analysis; contributes to the transparency of the project's development and intent" (OPC 2010, x).

In Australia's Victoria state, the Office of the Victorian Privacy Commissioner (OVPC) has produced "one of the three most useful guidance documents available in any jurisdiction, anywhere in the world" (Clarke 2012, 139). The current OVPC *PIA Guide* dates from April 2009 (OVPC 2009). It is the second edition of the guide originally published in August 2004. The OVPC *PIA Guide* is primarily aimed at the Victorian public sector, but it says it may assist anyone undertaking a PIA. The *Guide* says that public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence among members of the public that their privacy has been considered. Public consultation may generate new ideas for dealing with a policy problem. If wide public consultation is not an option, the *Guide* says the organization could consult key stakeholders who represent the project's client base or the wider public interest or who have expertise in privacy, human rights, and civil liberties.

In Canada, the Treasury Board Secretariat (TBS) issued PIA Guidelines in August 2002 (Treasury Board of Canada Secretariat 2002). It promulgated a new Directive on Privacy Impact Assessment in April 2010 (Treasury Board of Canada Secretariat 2010). The directive ties PIAs with submissions to the Treasury Board for program approval and funding. This is one of the strongest features of Canadian PIA policy. PIAs have to be signed off by senior officials, which is good for ensuring accountability, before a submission is made to the Treasury Board. The PIA is to be "simultaneously" provided to the Office of the Privacy Commissioner. Institutions are instructed to make parts of the PIA publicly available. Exceptions to public release are permitted for security as well as "any other confidentiality or legal consideration" (section 6.3.17).

In December 2010, Ontario's Office of the Information and Privacy Commissioner released a revised PIA guide, replacing the 2001 version. Three PIA tools were also released at that time and provide detailed instructions, checklists, templates, and other resources to help projects complete the PIA process. The *Privacy Impact Assessment Guide* for the Ontario Public Service says ultimate accountability for privacy protection rests with the Minister, as head of each government institution (OCIPO 2010). It states that "The potential damage to the individual must take precedence in your assessment over organizational risks" (OCIPO 2010, 48).

In 2001, the Office of the Information and Privacy Commissioner (OIPC) of Alberta introduced its first Privacy Impact Assessment (PIA) questionnaire. In January 2009, the OIPC revised the PIA template and guidelines (OIPC 2009). Not only are PIAs mandatory for health care projects, they must be submitted to the OIPC before implementation of a new system or practice. If the OIPC finds shortcomings, projects can be turned down or forced to make costly retrofits.

The Health Information and Quality Authority in Ireland is an independent authority, established under the Health Act 2007, to drive improvement in Ireland's health and social care services. Among other things, it aims to ensure that service users' interests are protected, including their right to privacy, confidentiality, and security of their personal health information. In December 2010, the Authority produced a PIA Guidance (Health Information and Quality Authority 2010a) following its review of PIA practice in other jurisdictions (Health Information and Quality Authority 2010b), which noted a growing convergence in what constitutes PIA best practice. The PIA Guidance says the primary purpose in undertaking a privacy impact assessment is to protect the rights of service users. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks. The Health Information and Quality Authority favours publication of PIA reports as it builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information. Completed PIA reports are to be presented in a reader-friendly format.

The origins of privacy impact assessment in New Zealand date back to at least 1993, to the legislative requirement under section 98 of the Privacy Act 1993 to undertake Information Matching Privacy Impact Assessments (IMPIAs) (Office of the Privacy Commissioner, 2008). The Office of the Privacy Commissioner (OPC) published a PIA Handbook in October 2002 (reprinted in 2007) (Office of the Privacy Commissioner 2007). It recommends that PIA reports be made publicly available, either in full or summary on an organization's website. The PIA Handbook mentions consultation with stakeholders but does not outline the consultative process. The agency conducting the PIA may consult the Privacy Commissioner. PIAs are generally not mandatory in New Zealand; however, Section 32 of the Immigration Act 2009 explicitly requires PIA to be conducted if biometric data are processed.

The Information Commissioner's Office (ICO) in the United Kingdom published a PIA handbook in December 2007 and became the first country in Europe to do so. The ICO published a revised version in June 2009 (Information Commissioner's Office 2009) and a streamlined version in August 2013.[3] The Cabinet Office, in its Data Handling Review, called for all central government departments to "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start" (Cabinet Office 2008, 18). It stressed that PIAs will be used and monitored in all departments. PIAs have thus become a "mandatory minimum measure" (Cabinet Office 2008a). The handbook places responsibility for managing a PIA at the senior executive level (preferably someone with responsibility for risk management, audit or compliance). The ICO emphasizes identification of and consultation with stakeholders in its Handbook.

In the United States, privacy impact assessments for government agencies are mandated under the E-Government Act of 2002. This act states that PIAs must be conducted for new or substantially changed programs that use personally identifiable information. Section 208 of the act requires that PIAs must be reviewed by a chief information officer or equivalent official, and should be made public, unless it is necessary to protect classified, sensitive, or private information. Agencies are expected to provide their director with a copy of the PIA for each system for which funding is requested. Each agency director must issue guidance to his or her agency specifying the contents required of a PIA.[4]

Additionally, the creation of the Department of Homeland Security (DHS) via the Homeland Security Act of 2002 mandates that the DHS conduct privacy impact

assessments and creates a Chief Information Officer position with responsibility for these privacy assessments.

On September 26, 2003, the U.S. Office of Management and Budget (OMB) issued a memorandum to heads of executive departments and agencies providing guidance for implementing the privacy provisions of the E-Government Act (Office of Management and Budget 2003). The OMB specifies what must be in a PIA and, in doing so, puts an implicit emphasis on the end product, the report, rather than on the process of conducting a PIA. Thus, we see that there are important differences in approach. Some favor or oblige publication of the PIA report, while others are silent on that prospect. Some favor consultation with external stakeholders, while for others that is not an issue. Some encourage or oblige third-party review or audit but most do not. Some are explicit in making senior officials responsible for the adequacy of a PIA but others are not. Much can be (and has been) learned from a review of these different methodologies in designing an optimized, more effective approach to PIA, as discussed later. The Irish and UK PIA handbooks both are based on extensive reviews of other PIA methodologies. Hence we can see a distinct evolution in the enhancement of the PIA process, which is also reflected (albeit briefly) in Article 33 of the proposed Data Protection Regulation.

PIAF PROJECT

The PIAF (PIAF stands for Privacy Impact Assessment Framework) consortium reviewed all of the PIA methodologies just described, as part of a project funded by the European Commission's Directorate-General Justice.[5] The PIAF project began in January 2011 and finished at the end of October 2012. The project had three main phases. In the first phase, the consortium examined the various PIA policies and methodologies, as already described, with a view to identifying the best elements of each. In the second phase, the consortium sent a survey to European data protection authorities asking for their views on some of the key elements and issues associated with PIA policy. In the third phase, the consortium prepared a set of recommendations on an optimized PIA framework based on their findings and conclusions from the previous phases.

Several data protection authorities said in their responses to the PIAF questionnaire that they preferred a streamlined, short, easy-to-understand and easy-to-use methodology. PIAF therefore produced a six-page "Step-by-step guide to privacy impact assessment" and a six-page "Template for a privacy impact assessment report."[6]

The consortium distinguished between a PIA *process* and a PIA *report*. A report is meant to document the PIA process, but in fact the PIA process extends beyond a PIA report. Even after the PIA assessor or team produces a report, which in most cases should contain recommendations, someone will need to make sure the recommendations are implemented or, if some are not, to explain why they are not.

Hence, the first document, the "Step-by-step guide," is a guide to the PIA process, while the other suggests what a PIA report should contain. The PIAF consortium prepared both documents based on their review of existing PIA methodologies as well as the contributions to the first and so far only book on privacy impact assessment, edited by two members of the consortium (Wright and De Hert 2012). The next section highlights the key elements in the optimized PIA process recommended by PIAF.

AN OPTIMIZED PIA METHODOLOGY

Drawing on the best practices of existing PIA methodologies, the "Step-by-step guide to privacy impact assessment" contains 16 principal steps in the "optimized" PIA process, as set out in this section. Some less than optimal PIAs may not follow all of these steps and some may follow them in variations of the sequence set out here. However, we regard the steps that follow as generally necessary if a PIA is to have "teeth," if the PIA is to be effective in identifying and minimizing or avoiding privacy risks. "Generally" is the operative word. If the privacy risk is regarded as relatively trivial, affecting only a few people, it may not be necessary to follow all of the steps set out here (e.g., it may not be necessary to consult external stakeholders or even to publish the PIA report). At the end of each step, we identify which countries promote such steps. The PIA *process* should always be distinguished from a PIA *report*. Production of a PIA report is only part of the PIA process, which continues even after the assessor has finished writing the report.

1. *Determine whether a PIA is necessary (threshold analysis).* Generally, if the development and deployment of a new project (or technology, service, etc.) impacts upon privacy, the project manager should undertake a PIA. A PIA should be undertaken when it is still possible to influence the design of a project or, if the project is too intrusive upon privacy, the organization may need to decide to cancel the project altogether rather than suffer from the negative reaction of consumers, citizens, regulatory authorities, the media and/or advocacy gadflies. Australia, Victoria state, Canada, Ontario, Alberta, Ireland, and the United States (DHS) use threshold analyses (typically a small set of questions) to determine whether a PIA should be conducted. The United Kingdom uses a threshold analysis to determine whether a "full-scale" or "small-scale" PIA should be conducted.

2. *Identify the PIA team and set the team's terms of reference, resources, and time frame*. The project manager should be responsible for the conduct of a PIA, but she or he may need some additional expertise, perhaps from outside her or his organization. The project manager and/or the organization's senior management should decide on the terms of reference for the PIA team. The terms of reference should spell out whether public consultations are to be held, to whom the PIA report is to be submitted, the nominal budget and time frame for the PIA, and whether the PIA report is to be published. The United Kingdom especially recommends this step. The minimum requirements for a PIA will depend on how significant an organization deems the privacy risks to be. That an organization may well downplay the seriousness of the risks makes third-party review and/or audit (see Step 14) necessary.
3. *Prepare a PIA plan*. The plan should spell out what is to be done to complete the PIA, who on the PIA team will do what, the PIA schedule, and, especially, how the consultation will be carried out. It should specify why it is important to consult stakeholders in this specific instance, who will be consulted, and how they will be consulted (e.g., via public opinion survey, workshops, focus groups, public hearings, online experience, etc.). Australia and the United Kingdom explicitly advocate preparation of plans for a PIA. Some countries, including Australia and the United Kingdom, say there is no "one size fits all" for PIA reports, while others, such as Alberta and Ireland, provide templates for such reports. If the regulator does not specify a PIA template, the author would encourage organizations to follow the PIA process advocated here and the PIA report template, which can be found on the PIAF website (see note 6).
4. *Agree on the budget for the PIA*. Once the project manager and/or assessor have prepared a PIA plan, they can estimate better the costs of undertaking the PIA and seek the budgetary and human resources necessary from the organization's senior management. Their plan may require an increase in the nominal budget initially set by senior management or the assessor may need to revise her or his PIA plan based on the budget available. If the assessor is unable to do an adequate PIA, she or he should note this in her or his PIA report.
5. *Describe the proposed project to be assessed*. The description can be used in at least two ways—it can be included in the PIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (why the project is being undertaken, who comprises the target market, how it might impact the citizen-consumer's privacy, what personal information will be collected). The project description should state who is responsible for the project. It should indicate important milestones and, especially, when decisions are to be made that could affect the project's design. All existing PIA methodologies include this step.
6. *Identify stakeholders*. The assessor should identify stakeholders, that is, those who are or might be interested in or affected by the project, technology, or service. The stakeholders could include people who are internal as well as external to the organization. They could include regulatory authorities, customers, citizen advocacy organizations, suppliers, service providers, manufacturers, system integrators, designers, academics, and so on. The assessor should identify these different categories and then identify specific individuals from within each of the categories, preferably as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy risks and the assumptions about the frequency and consequences of those risks and the numbers of citizen-consumers who could be impacted. Australia, Victoria state, Ireland, and the United Kingdom take this step.
7. *Analyze the information flows and other privacy impacts*. The assessor should consult with others in the organization and perhaps external to the organization to describe the information flows and, specifically, who will collect what information from whom for what purpose; how the organization will use the collected information; how the information will be stored, secured, processed, and distributed (i.e., to whom the organization might pass on the information), for what purpose, and how well will secondary users (e.g., the organization's service providers, apps developers) protect that information or whether they will pass it on to still others. This analysis should be as detailed as possible to help identify potential privacy risks. The assessor should consider the impacts not only on information privacy, but other types of privacy as well (Finn, Wright, and Friedewald 2013). Australia, Victoria state, Canada, Ontario, Alberta, Ireland, and New Zealand say that a PIA should describe information flows. This step could be taken immediately after Step 5 and concurrently with Step 6.
8. *Consult with stakeholders*. There are many reasons for doing so, not least of which is that they may identify some privacy risks not considered by the

project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream—when the project or technology or service is deployed—an adequate consultation at an early stage may help the organization avoid or minimise liability. Furthermore, consulting stakeholders may provide a sort of "beta test" of the project or service or technology. Consulted stakeholders are less likely to criticize a project than those who were not consulted. Australia, Victoria state, Ireland, and the United Kingdom urge consultation with stakeholders. This step could be taken after Step 5, but it would be better after Step 7, since the latter may uncover additional privacy risks not apparent after only Step 5.

9. *Check that the project complies with legislation*. A privacy impact assessment is more than a compliance check; nevertheless, the assessor or her/his legal experts should ensure that the project complies with any legislative or regulatory requirements. Australia, Victoria state, Canada, Ireland, New Zealand, the United Kingdom, and the United States note the importance of this step.
10. *Identify risks and possible solutions*. The assessor and her/his PIA team, preferably through stakeholder consultation, should identify all possible risks and whom those risks will impact and should assess those risks for their likelihood (frequency) and consequence (magnitude of impact), as well as the numbers of people who could be affected. Assessing risks is a somewhat subjective exercise. Thus, the assessor will benefit from engaging stakeholder representatives and experts to have their views. Deciding how to mitigate or eliminate or avoid or transfer the risk is also a somewhat political decision, as is the decision regarding which risks to retain. All PIA methodologies feature this step. Information security risks, such as those contained in ISO 27005 (ISO 2011), do not address specific privacy risks. Hence some PIA methodologies, for example, those of Australia, Victoria state, Canada Alberta, Ontario, and New Zealand, mention specific privacy risks, as does the privacy risk management methodology developed by the French data protection authority (CNIL 2012).
11. *Formulate recommendations*. The assessor should be clear to whom her/his recommendations are directed—some could be directed toward different units within the organization, some to the project manager, some to the chief executive officer (CEO), some to employees or employee representatives (e.g., trade unions), to regulatory authorities, third-party apps developers, and so on. If stakeholders have sight of draft recommendations, before they are finalized, they may be able to suggest improvements to existing recommendations or make additional ones. All PIA methodologies call for recommendations.
12. *Prepare and publish the report, for example, on the organization's website*. Some organizations may be afraid to publish their PIAs because they fear negative publicity or they have concerns about competitors learning something they don't want them to. There are solutions to such concerns. The organization can simply redact the sensitive bits or put them into a confidential annex or publish a summary of the PIA report. As in Step 11, if the assessor gives stakeholders sight of the draft PIA report, they may be able to suggest improvements before it is finalized. Australia and Ireland encourage publication, and the United States requires it. Canada publishes summaries.
13. *Implement the recommendations*. The project manager and/or the organization may not accept all of the PIA recommendations, but they should say which recommendations they are implementing and why they may not implement others. The organization's response to the assessor's recommendations should be posted on the organization's website. This transparency will show that the organization treats the PIA recommendations seriously, which in turn should show consumers and citizens that the organization merits their trust. Canada, Ireland, New Zealand, and the United Kingdom say a PIA report should justify any remaining risks. Victoria state says an organization will need to consider how residual risks will be managed.
14. *Third-party review and/or audit of the PIA*. Existing PIA reports are of highly variable quality, from the thoughtful and considered to the downright laughable. Some PIA reports exceed 150 pages, and others are only a page and a half in length, the sheer brevity of which makes them highly suspect. Independent, third-party review and/or audits are the only way to ensure PIAs are properly carried out and their recommendations implemented. The Office of the Privacy Commissioner of Canada has indicated and extolled the benefits of independent audits (Stoddart 2012). Data protection authorities do not have the resources to audit all PIAs, but they could audit a small percentage, enough to make organizations ensure their PIAs are reasonably rigorous. Alternatively, independent auditors could undertake this task, just as they audit a company's financial accounts. Yet another alternative would be for organizations such as the International Association of Privacy Professionals (IAPP) to certify

privacy auditors. The DHS has built independent, third-party review into its PIA process. The Office of the Privacy Commissioner audits PIAs in Canada. New Zealand also favours third-party review. The United Kingdom envisages review and audit of a PIA, but doesn't say who should do it.

15. *Update the PIA if there are changes in the project*. Many projects undergo changes before completion. Depending on the magnitude of the changes, the assessor may need to revisit the PIA as if it were a new initiative, including a new consultation with stakeholders. Australia says a PIA may need to be revisited as a project progresses. So do Ontario, the United Kingdom, and the U.S. Office of Management and Budget (OMB).
16. *Embed privacy awareness throughout the organization and ensure accountability.* The chief executive officer is responsible for ensuring that all employees are sensitive to the privacy implications, the possible impacts on privacy, of what they or their colleagues do. The CEO should be accountable to her/his supervisory board or shareholders for the adequacy of PIA. In Canada, PIA reports have to be signed off by a senior official (e.g., a deputy minister). Ireland also says PIA reports should be approved by senior management. In the United States, the chief information officer or privacy officer is expected to review and sign off PIAs. Some PIA methodologies (e.g., Canada) explicitly say that organizations should provide guidance and training to managers and staff.

BENEFITS

Some might see the cost and time needed to conduct a PIA as reasons not to do a PIA or to do PIA in the most cursory fashion possible. Certainly, it is true that the cost and time needed will vary significantly, depending on the complexity and seriousness of the privacy risks. However, the costs of fixing a project (using the term in its widest sense) at the planning stage will be a fraction of those incurred later on. If the privacy impacts are unacceptable, the project may even have to be cancelled altogether. Thus, a PIA helps reduce costs in management time, legal expenses, and potential media or public concern by considering privacy issues early. It helps an organization to avoid costly or embarrassing privacy mistakes. It provides a way to detect potential privacy problems, take precautions, and build tailored safeguards before, not after, the organization makes heavy investments.

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

A PIA enhances informed decision making and exposes internal communication gaps or hidden assumptions about the project. A PIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision-makers. A PIA can be a credible source of information. It enables an organization to learn about the privacy pitfalls of a project directly, rather than having its critics or competitors point them out.

A PIA can help an organization to gain the public's trust and confidence that privacy has been built into the design of a project, technology, or service. Trust is built on transparency, and a PIA is a disciplined process that promotes open communications, common understanding, and transparency. Customers or citizens are more likely to trust an organization that performs a PIA than one that does not. They are more likely to take their business to an organization they can trust than one they don't.

An organization that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them to do so too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that might damage the organization. It is a way to affirm the organization's values. An organization may wish to use a PIA as a way to check out third-party suppliers, to verify that they will not create privacy problems. A proper PIA also demonstrates to an organization's customers and/or citizens that it respects their privacy and is responsive to their concerns.

We assume regulators are likely to be more sympathetic toward organizations that undertake PIAs than those that do not. A PIA is a self- or co-regulatory instrument that may obviate the need for "hard" law. Thus, if organizations are seen to carry out proper ("full-blooded") PIAs, they may escape the more onerous burdens imposed by legislation.

CONCLUSION

Article 33 and comments of the Article 29 WP suggest that the EC and data protection authorities, acting collectively, are on the right track with regard to the establishment of privacy impact assessment as an important new tool in shoring up privacy against the depredations and intrusions of corporate warlords and arrogant or unthinking bureaucrats.

However, more specificity is needed in promulgating a PIA process across Europe before the new Data Protection Regulation is adopted. The most controversial elements

in a PIA process are engaging stakeholders, publishing the PIA report, and subjecting the PIA report to third-party review or an audit. The elements in our proposed PIA methodology, especially the controversial ones, are necessary to make a PIA meaningful, to give it teeth, and forestall reduction of a PIA into a whitewash exercise. The benefits of a proper PIA have been outlined elsewhere (see Wright 2012). These benefits need to be promoted as a counter to the efforts of lobbyists to water down the EC's proposed legislation.

If Europe adopts an optimized PIA, drawing on the experience of the countries discussed in the preceding sections and as outlined in the 16 steps mentioned here, it will set a new high-water mark in protecting privacy, one that can be emulated by other countries as they too begin to formulate PIA policies and methodologies.

NOTES

1. More detailed information on these countries can be found in Wright et al. (2011) and Wright and De Hert (2012). Chapter 1 ("Introduction to Privacy Impact Assessment") of Wright and De Hert (2012) contains a systematic comparison of different PIA methodologies.

2. The Privacy Commissioner acknowledges (Office of the Victorian Privacy Commissioner 2009) that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence, or, for private-sector organizations, other competitive reasons for not making a PIA public in full or in part. However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the commissioner encourages organizations to consider the release of a summary version.

3. The streamlined version was expected to be made public in mid August 2013. However, it was not available at the time this article went to press. Hence, all references in this article are to the second edition of the ICO PIA Handbook.

4. E-government Act of 2002, Pub.L.107–347.

5. The PIAF consortium comprises Vrije Universiteit Brussel (Belgium), Trilateral Research & Consulting (UK), and Privacy International (UK). In addition to a review of PIA methodologies, the PIAF report includes an analysis of 10 PIA reports, two each from Australia, Canada, New Zealand, the United Kingdom, and the United States. To our knowledge, this is the first such review of actual PIA reports from these countries.

6. Both papers can be found here: http://www.piafproject.eu/Events.html (accessed June 22, 2013).

REFERENCES

Article 29 Data Protection Working Party. 2012. Opinion 01/2012 on the data protection reform proposals, Brussels, 23 March. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf (accessed June 22, 2013).

Cabinet Office. 2008a. Cross government actions: Mandatory minimum measures. http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf (accessed June 22, 2013).

Cabinet Office. 2008b. Data handling procedures in government: Final report. June. http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf (accessed June 22, 2013).

Clarke, R. 2012. PIAs in Australia: A work-in-progress report. In *Privacy impact assessment*, ed. David Wright and Paul de Hert, 119–48. Dordrecht, The Netherlands: Springer.

Commission Nationale de l'Informatique et des Libertés (CNIL), Methodology for Privacy Risk Management, Paris. 2012. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf (accessed June 22, 2013).

European Commission. 2012. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final, Brussels, 25 January. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (accessed June 22, 2013).

Finn, R., D. Wright, and M. Friedewald. 2013. Seven types of privacy. In *European data protection: Coming of age?*, ed. S. Gutwirth, R. Leenes, P. De Hert, et al., 3–32. Dordrecht, The Netherlands: Springer.

Health Information and Quality Authority. 2010a. *Guidance on privacy impact assessment in health and social care*. Dublin, December. http://www.hiqa.ie/resource-centre/professionals (accessed June 22, 2013).

Health Information and Quality Authority. 2010b. *International review of privacy impact assessments*. http://www.hiqa.ie/standards/information-governance/health-information-governance (accessed June 22, 2013).

Information Commissioner's Office. 2009. *privacy impact assessment handbook*, Version 2.0. Cheshire, UK: Wilmslow. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html (accessed June 22, 2013).

International Organization for Standardization. 2011. *Information technology—Security techniques—Information security risk management, ISO/IEC 27005:2011, Second edition*, Geneva, 1 June. http://www.iso.org/iso/catalogue_detail?csnumber=56742 (accessed June 22, 2013).

Office of Management and Budget. 2003. *OMB guidance for implementing the privacy provisions of the E-Government Act of 2002*. Washington, DC, September 26. http://www.whitehouse.gov/omb/memoranda/m03–22.html (accessed June 22, 2013).

Office of the Chief Information and Privacy Officer. 2010. *Privacy impact assessment guide for the Ontario Public Service*. Toronto: Queen's Printer for Ontario.

Office of the Information and Privacy Commissioner of Alberta. 2009. *Privacy impact assessment (PIA) requirements*, For use with the Health Information Act. January. www.OIPC.ab.ca (accessed June 22, 2013).

Office of the Privacy Commissioner. 2008. Guidance note for departments seeking legislative provision for information matching, 16 May, Appendix B. http://privacy.org.nz/guidance-note-for-departments-seeking-legislative-provision-for-information-matching/#appendix (accessed June 22, 2013).

Office of the Privacy Commissioner. 2007. *Privacy impact assessment handbook*. Auckland/Wellington. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf (accessed June 22, 2013).

Office of the Privacy Commissioner. 2010. *Privacy impact assessment guide*. Sydney, NSW, August 2006, revised May. http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide (accessed June 22, 2013).

Office of the Victorian Privacy Commissioner. 2009. Privacy impact assessments—A guide for the Victorian public sector, Edition 2, Melbourne, April. http://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/pages/guidelines (accessed June 22, 2013).

Stoddart, Jennifer. 2012. Auditing privacy impact assessments: The Canadian experience. In *Privacy impact assessment*, ed. D. Wright and P. de Hert, 419–36. Dordrecht, The Netherlands: Springer.

Treasury Board of Canada Secretariat. 2002. *Privacy impact assessment guidelines: A framework to manage privacy risks*. Ottawa, August 31. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp (accessed June 22, 2013).

Treasury Board of Canada Secretariat. 2010. Directive on privacy impact assessment. Ottawa, April 1. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text#cha1 (accessed June 22, 2013).

Wright, D. 2012. The state of the art in privacy impact assessment. *Computer Law & Security Review* 28(1): 54–61.

Wright, D., K. Wadhwa, P. De Hert, and D. Kloza. 2011. PIAF deliverable D1, September. http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf (accessed June 22, 2013).

Wright, D., and P. De Hert, eds. 2012. *Privacy impact assessment*. Dordrecht, The Netherlands: Springer.

Wright, D., R. Finn, and R. Rodrigues. 2013. A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research* 9(1): 160–80.