Chapter 1
Introduction to Privacy Impact Assessment

David Wright and Paul De Hert

1.1 Growing Interest

If privacy is a cornerstone of democracy,[1] then democracy is in trouble. Especially since the advent of the computer, the encroachments on privacy have proliferated. Terrorist attacks in the early 21st century have given governments all the justifications they need to bolster national security by forcing telecom companies to retain telephone records, to justify warrantless eavesdropping on our phone calls, to examine our bank records, to fuse personally identifiable information from multiple sources, to profile citizens to determine who presents a risk to the established order. Many companies have either aided and abetted governmental efforts or engaged in their own surreptitious amassing of the details of our lives. Personal data in real time has become the fuel of today's economy. The development of new technologies, while indisputably offering many benefits, is the proverbial two-edged sword: it cuts both ways, and if the wielder is not careful, he may suffer more than superficial lacerations. Technologies can be and are employed to discover more about where we are, where we go, what we are doing, what are our interests and proclivities, to manipulate our behaviour and choices in ways of which most people are not aware and, if they are, are powerless against the inexorable lust for personal data. It comes as no surprise that many would-be jeremiahs have already pronounced privacy is dead. Indeed, many of those who would like to preside over the last rites are the very people who stand to profit most from the burial of this fundamental right.

[1] The Supreme Court of Canada has stated that "society has come to realize that privacy is at the heart of liberty in a modern state . . . Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual". R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.). Also: "Without privacy, it is much harder for dissent to flourish or for democracy to remain healthy and robust. Equally, without privacy the individual is always at the mercy of the state, forced to explain why the government should not know something rather than being in the position to demand why questions are being asked in the first place." Goold, Benjamin J., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009.

D. Wright (✉)
Trilateral Research & Consulting, London, W8 5JB, UK
e-mail: david.wright@trilateralresearch.com

D. Wright, P. De Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, DOI 10.1007/978-94-007-2543-0_1,

But privacy is not dead. Opinion polls consistently show unease and distrust of our political leaders and the corporate warlords on matters of privacy. Citizens may choose to forego personal details, at the relentless urging of big business, but they still value what they have left.

One of the instruments for safeguarding privacy is privacy impact assessment (PIA). There is growing interest in PIA and, consequently, it seems timely to publish what we believe is the first book on the subject.

In Europe, the interest in PIA has been sparked by two main events. First was development and publication of a PIA handbook in the UK, the first in Europe, in December 2007.[2] Second was the European Commission's Recommendation on RFID in May 2009 in which the Commission called upon the Member States to provide inputs to the Article 29 Data Protection Working Party for development of a privacy impact assessment framework for the deployment of radio frequency identification (RFID) tags.

Article 4 of the European Commission's Recommendation on RFID said, "Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union."[3] The RFID PIA Framework, developed by industry, was endorsed by the Art. 29 Working Party in February 2011.

Since these two milestones, there have been frequent calls for PIA in Europe. The European Parliament, in its 5 May 2010 resolution on passenger name records (PNR), said that "any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test".[4]

European Commission Vice-President Viviane Reding said in July 2010 that "Businesses and public authorities... will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach."[5]

---

[2] Information Commissioner's Office (ICO), *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, December 2007, Version 2.0, June 2009.

[3] European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

[4] European Parliament, Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN

[5] Reding, Viviane, Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship, "Towards a true Single Market of data protection", SPEECH/10/386, Meeting of the Article 29 Working Party re "Review of the Data protection legal

In its Communication of 4 November 2010, the European Commission said it will examine the possibility of including in its proposed new legal framework on data protection "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".[6]

The exact wording of the new data protection legislation in Europe remains to be seen, but the Commission's Communication seems to indicate that PIAs would be required of all data controllers, not just those from public institutions, but also from the private sector. Neelie Kroes, Vice-President of the European Commission for the Digital Agenda, pointed in this direction in April 2011 when she said the RFID PIA Framework "constitutes an interesting model that could be used for other similar situations or areas, such as smart metering and online behavioural advertising". She also said that the PIA Framework was "potentially also the start of a new policy approach, in fact a new commitment to involving all stakeholders in the process of solving privacy problems".[7]

In any event, although PIAs have been used mainly by governments, the private sector is also taking an interest in PIAs, as the chapters on Nokia, Siemens and Vodafone in this book make clear.

1.2 A Few Key Definitions

As the term suggests, a *privacy impact assessment* is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts.

A PIA is more than a tool: it is a *process* which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been

framework", Brussels, 14 July 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386

[6] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (2010) 609 final, Brussels, 4 Nov 2010, p. 12. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

[7] She also said that "the European Commission has issued a mandate to the European Standards organisations CEN and ETSI to assess if a translation of the PIA Framework into a standard is feasible." Kroes, Neelie, "Smart tags – working together to protect privacy", SPEECH/11/236, at the Privacy and Data Protection Impact Assessment Framework Signing Ceremony, Brussels, 6 April 2011. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/236&format=HTML&aged=0&language=en&guiLanguage=en

deployed. A good PIA will engage stakeholders from the outset as a way of gathering their views and ideas about how any intrusive privacy impacts can be avoided or mitigated.

Although PIAs are not used in many countries, the term has been defined in various ways[8] and the methodology employed, as this book makes clear, differs from one regime to another, from one company to another. Here are some examples:

Roger Clarke, one of the earliest proponents of PIAs and author of the chapter on Australia in this book, has defined a privacy impact assessment as "a systematic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts".[9]

The Australian PIA Guide says a privacy impact assessment is more than a compliance check. In addition to checking a project's compliance with legislation, regulations, codes of practice, etc., a PIA investigates how information flows affect individuals' choices, the degree of intrusiveness into individuals' lives, how the project fits into community expectations.[10]

Deloitte and Touche defined a PIA as "a process to help determine whether technologies, information systems and proposed programs or policies meet privacy requirements. It measures both technical compliance with privacy legislation and the broader privacy implications of a given proposal, project or product."[11]

The Hong Kong Office of the Privacy Commissioner for Personal Data defined PIA as "a systematic process that evaluates proposed initiatives or strategic options in terms of their impact upon privacy. To be effective a PIA needs to be an integral part of the project planning process rather than an afterthought. The purpose of this assessment is twofold:

- To identify the potential effects that a project or proposal may have upon personal data privacy e.g., the introduction of a multi-purpose smart card.
- Secondly, to examine how any detrimental effects upon privacy might be mitigated."[12]

---

[8] Clarke, Roger, "Privacy Impact Assessment: Its Origins and Development", *Computer Law & Security Review*, Vol. 25, No. 2, April 2009, pp. 123–135. PrePrint at http://www.rogerclarke.com/DV/PIAHist-08.html

[9] Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, 2011. http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full or http://www.rogerclarke.com/DV/PIAG-Eval.html

[10] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, Sydney, NSW, August 2006, revised May 2010, p. xxxvii. http://www.privacy.gov.au. On 1 November 2010, the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner (OAIC).

[11] Karol, Thomas J., "Cross-Border Privacy Impact Assessments: An Introduction", *ISACA Journal*, Vol. 3, 2001. http://www.isaca.org/Journal/Past-Issues/2001/Volume-3/Pages/Cross-Border-Privacy-Impact-Assessments.aspx.

[12] See point 8.3 on this web page: http://www.pcpd.org.hk/english/publications/eprivacy_9.html

The New Zealand PIA Handbook defines a PIA similarly, as "a systematic process for evaluating a proposal in terms of its impact upon privacy," the purpose of which is to:

- identify the potential effects that the proposal may have upon personal privacy
- examine how any detrimental effects on privacy might be lessened.

A PIA can be used "to inform decision-makers about whether a project should proceed and, if so, in what form".[13]

Canada's PIA Guidelines define a PIA as "a process to determine the impacts of a proposal on an individual's privacy and ways to mitigate or avoid any adverse effects".[14]

The Alberta Office of the Information and Privacy Commissioner describes a PIA as "a due diligence exercise, in which the organization identifies and addresses potential privacy risks that may occur in the course of its operations".[15]

The US Office of Management and Budget (OMB) defines PIA as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."[16]

The US Department of Homeland Security (DHS) defines PIA as "a vital tool that evaluates possible privacy risks and the mitigation of those risks at the beginning of and throughout the development life cycle of a program or system".[17]

Thus, although the wording of the definitions differs, there is considerable similarity in the principal ideas conveyed, i.e., that PIA is a process for identifying and evaluating risks to privacy, checking for compliance with privacy legislation and considering ways in which those risks can be avoided or mitigated.

Here, more briefly, are a few other key definitions:

Data protection impact assessment – The European Commission has been using this term. It appears in its RFID Recommendation and, later, in its 4 November 2010 Communication on revision of the Data Protection

[13] Stewart, Blair, *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, March 2002, revised June 2007, pp. 5, 9. The similarity is not coincidental. Blair Stewart drafted both the Hong Kong and New Zealand handbooks.

[14] Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, Ottawa, 31 August 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp

[15] http://www.oipc.ab.ca/pages/PIAs/Description.aspx

[16] http://www.whitehouse.gov/omb/memoranda_m03-22

[17] Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance*, Washington, DC, June 2010. http://www.dhs.gov/files/publications/gc_1209396374339.shtm

Directive. Paul De Hert in Chapter 2 of this book equates "data protection impact assessments with simply checking the legal requirements spelled out in the European data protection framework", i.e., a data protection impact assessment is primarily a compliance check and, therefore, somewhat restricted in scope compared to a PIA.

Compliance check – A compliance check is to determine whether a project complies with relevant legislative and/or regulatory requirements. It might also check with relevant codes of practice, industry and/or community standards or ethical guidelines. A compliance check may be carried out at the beginning or during or following completion of a project.

Privacy audit – A privacy audit checks to see that PIA recommendations have been implemented and/or how effective privacy safeguards are. "An audit is undertaken on a project that has already been implemented. An audit is valuable in that it either confirms that privacy undertakings and/or privacy law are being complied with, or highlights problems that need to be addressed."[18]

Prior checking – This term has its origins in article 20 of the EU Data Protection Directive (95/46/EC) which says 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." See Chapter 4 by Gwendal Le Grand and Emilie Barrau for more on prior checking.

Project – Here we use the term "project" as short-hand for any project, policy, program, service, system, technology or other initiative involving the processing of personal information or impacting privacy. A project can refer to a new initiative or changes to an existing project.[19]

1.3 A PIA Timeline

Privacy impact assessment may seem to be a new instrument in Europe, but, in fact, PIAs have been used for quite some time in other parts of the world. David Flaherty, former Information and Privacy Commissioner of British Columbia, said he could document use of the term "privacy impact statement" as early as the 1970s.[20] The Treasury Board of Canada Secretariat also claims that PIAs have been used as far back as the 1970s.[21]

---

[18] ICO, *PIA Handbook*, op. cit., p. 3.

[19] ICO also uses the term "project" in a wide sense: "The term 'project'…. could equally refer to a system, database, program, application, service or a scheme, or an enhancement to any of the above, or an initiative, proposal or a review, or even draft legislation." UK, *PIA Handbook*, op. cit., p. 2.

[20] See endnote 3 in Flaherty, David, "Privacy Impact Assessments: An Essential Tool for Data Protection", *Privacy Law and Policy Reporter*, Vol. 7, No. 5, November 2000. http://www.austlii.edu.au/au/journals/PLPR/2000/

[21] http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-3-eng.asp

Table 1.1 provides a timeline of key PIA guidance documents.

Table 1.1 Milestones in the development of PIA methodologies

Year	Milestones
1996	The **US** Internal Revenue Service issues its IRS Privacy Impact Assessment.[22] The Federal Chief Information Officers Council endorses it as a "best practice" in 2000.
1999	**Ontario**'s Management Board Secretariat (MBS), now part of the Ministry of Government Services, releases PIA Guidelines requiring provincial government ministries to accompany proposals for new Information and IT projects with PIAs.[23]
2001	**Hong Kong**'s Office of the Privacy Commissioner for Personal Data publishes an Information Book, a chapter of which is devoted to "E-Privacy Strategic Planning and privacy Impact Assessment".
	Deloitte and Touche publishes *A Guide To Cross-Border Privacy Impact Assessments*.
	Ontario's Management Board Secretariat (MBS), Information and Privacy Office, publishes *Privacy Impact Assessment: a User's Guide*. The Ministry of Government Services issues a *PIA Screening Tool* (undated).
	Alberta requires PIAs under its Health Information Act which comes into effect in April.[24]
2002	The **New Zealand** Office of the Privacy Commissioner publishes its *Privacy Impact Assessment Handbook* in March 2002, which is later revised in 2007.
	The Treasury Board of **Canada** Secretariat publishes its *Privacy Impact Assessment Policy* and *PIA Guidelines: A Framework to Manage Privacy Risks*.
	The **US** signs into law the E-Government Act, section 208 of which calls for PIA.
2003	The US Office of Management and Budget (OMB) issues "E-Government Act Section 208 Implementation Guidance".
	The Treasury Board of **Canada** Secretariat publishes a *Report on PIA Best Practices* and its *PIA e-learning tool*.
2004	The Treasury Board of **Canada** Secretariat publishes a Privacy Impact Assessment Audit Guide.
	The Victorian Privacy Commissioner in Australia publishes a PIA guide, which is significantly amended in 2009, such that Roger Clarke describes it as one of the three most useful in the world.[25]
	The **US DHS** issues its PIA guidance document *Privacy Impact Assessments Made Simple*. It issues a revised *Privacy Impact Assessment Guidance* in 2006, 2007 and 2010.[26]

[22] Internal Revenue Service, *IRS Privacy Impact Assessment, Version 1.3*, Washington, DC, 17 December 1996. www.cio.gov/documents/pia_for_it_irs_model.pdf

[23] Memo dated 16 December 1999 from D. Scott Campbell, MBS Corporate Chief Information Officer, to government Chief Information Officers, Chief Administrative Officers, IT Directors.

[24] Waters, Nigel, "'Surveillance-Off': Beyond Privacy Impact Assessment – Design Principles to Minimize Privacy Intrusion", Paper for the 16th Annual Privacy Laws and Business International Conference: *Transforming Risk Assessment into Everyday Compliance with Data Protection Law*, St John's College, Cambridge, England, 7–9 July 2003.

[25] See Chapter 5. The other two appreciated by Clarke are the UK ICO PIA Handbook and Ontario's PIA User's Guide.

[26] DHS, *PIAs: The Privacy Office Official Guidance*, op. cit.

Table 1.1 (continued)

Year	Milestones
2006	**Australia**'s Office of the Privacy Commissioner publishes its *Privacy Impact Assessment Guide.* A revised version is published in 2010. The **British Columbia** Ministry of Labour and Citizens' Services issues its *Privacy Impact Assessment Process*.
2007	The **UK** Information Commissioner's Office publishes its *Privacy Impact Assessment Handbook*, in December. A revised version is published in June 2009.
2008	The **International Organization for Standardization** (ISO) publishes its PIA standard 22307:2008 Financial services – Privacy impact assessment.
2009	On 12 May, the **European Commission** releases its Recommendation on RFID in which advocates a "privacy and data protection impact assessment".
2010	In July, the Treasury Board of **Canada** Secretariat issues its Directive on Privacy Impact Assessment, which supersedes its PIA Policy from 2002.
2011	In February, the **Art. 29 Working Party** approves an RFID PIA Framework developed by an industry group.

1.4 Why Carry Out a PIA?

Why carry out a PIA? There are various reasons why organisations, both governmental and business, carry out a PIA. In some cases, as in Canada, the US and perhaps the UK, they are mandatory for government departments and agencies. In other cases, organisations carry out a PIA because they want to avoid or manage risks and gain certain benefits.

1.4.1 To Manage Risks

A PIA should be methodologically based on a risk assessment and management process.[27] If a government agency or company or any entity dealing with personal data can avoid implementing a privacy-intrusive scheme, it will minimise downstream risks. PIA proponents have identified various risks to an organisation that collects or processes personally identifiable information and various benefits flowing from the conduct of a PIA to identify, avoid or mitigate those risks. Indeed, many of them see PIA as fitting into the organisation's overall risk management strategy. For example, Australia's Guide says: "PIA information feeds into broader project risk management processes."[28] Privacy risks may flow from any number of sources. Risks may arise from vulnerabilities within the organisation or the design and implementation

[27] The authors would like to thank Barbara Daskala of ENISA for her useful comments and suggestions on section 1.4 of this chapter.

[28] OPC, *PIA Guide*, op. cit., p. vii. The ICO PIA Handbook (p. 5) makes the same point: "Risk management has considerably broader scope than privacy alone, so organisations may find it appropriate to plan a PIA within the context of risk management."

of a project. They may also arise from external threats, e.g., from evil-doers who engage in social engineering to con personnel into giving them the information they want or who exploit weaknesses in the organisation's access control procedures. Virtually all PIA guides used in Australia, Canada, New Zealand, the UK and the US identify risks facing an organisation associated with the collection and processing of personal identifiable information.

We need to be a bit more precise about these "risks". It is useful to distinguish between vulnerabilities of assets, threats and risks, as the European Network and Information Security Agency (ENISA) does in its risk assessments of new information and communications technologies. ENISA defines a risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization",[29] which is virtually identical to that used in the ISO 27005 standard upon which ENISA draws. If we accept the ISO's terminology, many of the "risks" in the PIA literature are actually threats or vulnerabilities.

1.4.1.1 Assets

According to the ISO/IEC 27005:2008 standard, an asset is anything that has value to an organisation and which therefore requires protection. The identification of the assets is a complex and challenging exercise but very important, since this will provide the basis on which assessment of the impacts and risks will be performed. The asset identification should be ideally performed at a suitable level of detail and according to the needs and the scope of the risk assessment.

Assets can be business processes and activities, information or hardware and software components, network, personnel, etc.

The asset is also valuated, since its value is a determinant in the estimation of the impact of a security incident. There are many different approaches that can be followed in order to do that; a very common basis for assets valuation is to consider the costs incurred due to the breach of confidentiality, integrity and availability as the result of an incident.

1.4.1.2 Vulnerabilities

A "vulnerability" refers to an aspect of a system or process (the assets) that can be exploited for purposes other than those originally intended, to weaknesses, security holes or implementation flaws within a system that are likely to be threatened. A

[29] http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/glossary. ENISA's definition of a risk is virtually identical to that in the ISO 27005 standard which defines an "information security risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and its consequence." International Organization for Standardization (ISO), *Information Technology – Security Techniques – Information Security Risk Management*, International Standard, ISO/IEC 27005:2008(E), First edition, 15 June 2008, p. 1.

vulnerability does not cause harm in itself[30]: to be considered a risk, a vulnerability needs to be exploited by a threat. In addition, vulnerabilities are independent of any particular threat. Understanding vulnerabilities is an important part of estimating risk. Vulnerabilities can increase risk, either by influencing the likelihood of some event or the severity of the consequences, should it occur, or both. Decisions about how to manage risks must also include consideration of ways to reduce vulnerabilities.[31]

Here are some examples of different types of vulnerabilities:

- Hardware – unprotected storage of personal data
- Software – insufficient testing of software or inadequate user authentication mechanism
- Network – unprotected communication lines
- Personnel – inadequate screening of new recruits or insufficient training
- Site – inadequate physical security (doors, windows)
- Organisation – lack of regular, third-party audits, lack of procedures for introducing software into operational systems, lack of records in administrator and operator logs.[32]

1.4.1.3 Threats

A threat has the potential to harm or compromise assets such as information, processes and systems and therefore organisations. Threats may be of natural or human origin, and could be accidental or deliberate. A threat may arise from within or from outside the organisation.[33] Physical or environmental threats such as a fire, an earthquake, a flood or a failure in the power supply or in telecommunications equipment may result in damage to computers, servers and networks used by an organisation to store or process personal data.

Personal data may also be *compromised* by other threats such as the following:

- Interception of communications
- Spying
- Theft of equipment, such as mobile phones, laptops, memory sticks, documents or data (identity theft)

---

[30] International Organization for Standardization (ISO), *Information Technology – Security Techniques – Information Security Risk Management*, International Standard, ISO/IEC 27005:2008(E), First edition, 15 June 2008, p. 13.

[31] Renn, Ortwin, *Risk Governance*, Earthscan, London, 2008, p. 69.

[32] For a much longer list of examples of vulnerabilities, see ISO/IEC 27005:2008(E), op. cit., pp. 42–45.

[33] For example, an employee of phone operator T-Mobile sold thousands of customer records to rivals. See Wray, Richard, "T-Mobile Confirms Biggest Phone Customer Data Breach", *The Guardian*, 17 November 2009. http://www.guardian.co.uk/uk/2009/nov/17/t-mobile-phone-data-privacy

- Retrieval of recycled or discarded media ("dumpster diving")
- Disclosure – such as AOL's disclosure of what it thought was anonymised data[34]
- Data from untrustworthy sources
- Tampering with hardware or software, including viruses and other malware[35]
- Position detection – Mobile phone companies are able to detect where we are more or less continuously[36]
- Unauthorised use of equipment or illegal processing of data
- Loss of data, e.g., through network failure or human error[37]
- Powerful new Internet technologies[38]
- Function creep, where data collected for one purpose is used for another purpose not previously specified.

Based on the above, the difference between a vulnerability, threat and risk can be illustrated thusly: An unprotected communications line is a vulnerability. Someone eavesdropping on that line is a threat. The risk is the probability that someone will actually do so and the consequence, the harm that will result. The risk may be minor – two teenagers discussing their homework assignment for tomorrow – or major, for example, a prime minister is recorded discussing his frolics with his teenage mistress. Here's another example: An organisation may not encourage employees to use strong passwords (a vulnerability). A hacker who can easily guess a simple password is a threat. The risk is the probability that he will do so and the consequence that may have for the organisation if he does so. Determining the risk(s) resulting from various vulnerabilities and threats requires some analysis and assessment, which is what a PIA can and should do.

---

[34] Barbaro, Michael, and Tom Zeller Jr, "A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times*, 9 August 2006. http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63

[35] See, for example, BBC News, "Sites Hit in Massive Web Attack", 2 April 2011. http://www.bbc.co.uk/news/world-us-canada-12944626

[36] "Cellphone companies do not typically divulge how much information they collect, so Mr. Spitz went to court to find out exactly what his cellphone company, Deutsche Telekom, knew about his whereabouts. The results were astounding. In a 6-month period – from August 31, 2009, to February 28, 2010, Deutsche Telekom had recorded and saved his longitude and latitude coordinates more than 35,000 times." Cohen, Noam, "It's Tracking Your Every Move and You May Not Even Know", *The New York Times*, 26 March 2011. http://www.nytimes.com/2011/03/26/business/media/26privacy.html

[37] For example, British tax authorities lost two computer disks with the personal data of 25 million people in October 2007. See Pfanner, Eric, "Data Leak in Britain Affects 25 Million", *The New York Times*, 22 November 2007. http://www.nytimes.com/2007/11/22/world/europe/22data.html?hp

[38] "Worries over Internet privacy have spurred lawsuits, conspiracy theories and consumer anxiety as marketers and others invent new ways to track computer users on the Internet. But the alarmists have not seen anything yet. In the next few years, a powerful new suite of capabilities [referring to HTML 5] will become available to Web developers that could give marketers and advertisers access to many more details about computer users' online activities." Vega, Tanzina, "Web Code Offers New Ways To See What Users Do Online", *The New York Times*, 10 October 2010. http://www.nytimes.com/2010/10/11/business/media/11privacy.html?src=busln

1.4.1.4 Impact Assessment

A PIA should not only consider the impacts on privacy, but also the impacts on an organisation flowing from the compromise of privacy. Many organisations have scant regard for privacy, so convincing them of the merits of PIA may require a focus on the impacts of comprised privacy on the organisation itself. Impacts may be either direct or indirect. An organisation risks suffering various consequences from not taking adequate care of the personal data in its possession, including the following direct impacts:

- Negative media attention
- Loss of customer confidence, loss of credibility, damage to trust and reputation leading to a loss of electoral support or a loss of customers and/or suppliers[39]
- Infringement of laws and/or regulations leading to judicial proceedings and penalties or the imposition of new regulatory controls in response to public concerns about the project, which could result in unforeseen or unexpected costs to the organisation.
- Direct financial loss from fines or penalties[40]
- Dismissal or resignations of senior personnel[41]

---

[39] See, for example, Schich, Kathrin, "Axel Springer hit by New German Data Leak Scandal", *Reuters*, 19 October 2008. http://uk.reuters.com/article/internetNews/idUKTRE49H1GN20081019

[40] Culnan and Williams provide two examples:

- After ChoicePoint failed in its credentialing procedures enabling criminals masquerading as small business to gain access to customer accounts, the company had to send letters to 145,000 individuals notifying them that their personal information had been fraudulently accessed and used to commit identity theft. ChoicePoint costs have been estimated at $30 million including fines of $10 million plus $5 million to create a fund for consumer redress. In addition, ChoicePoint was required to undergo biennial independent assessments for 20 years and provide copies to the Federal Trade Commission upon request.
- US retailer TJX was faulted for storing unencrypted sensitive information, failing to limit unauthorised wireless access to its networks, and failing to employ appropriate security measures on its networks, which enabled criminals to access 45 million records. Costs to TJX have been estimated at $156 million including $40.9 million to Visa and $24 million to MasterCard to cover fraud losses.

Culnan, Mary J., and Cynthia Clark Williams, "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches", *MIS Quarterly*, Vol. 33 No. 4, December 2009, pp. 673–687. Re the cost of a data breach, see also Espiner, Tom, "Data Breaches Cost an Average Business £1.4m", ZDNet.co.uk, 25 February 2008. http://news.zdnet.co.uk/security/0,1000000189,39341215,00.htm

[41] See, for example, *The Inquirer*, "Head taxman quits after 25 million peoples' data lost", 20 November 2007. http://www.theinquirer.net/gb/inquirer/news/2007/11/20/head-taxman-quits-million. See also Richards, Jonathan, "Top Officials to be Held to Account for Data Losses", *The Times*, 22 April 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/article3797278.ece

- Retrofits or redesigns of projects[42] or outright cancellation of a project[43]
- Unexpected or untoward consequences as a result of erroneous personal data, for example, some people may be prosecuted or falsely accused or under suspicion or may suffer unduly (e.g., they are on a "no-fly list" or cannot enter a country or are turned down for a job) because the personal data held by the organisation is incorrect.

Examples of indirect impacts include

- Opportunity costs – The time an organisation spends in fixing a compromise of personal data is time that could have been spent on growing the business
- Loss of a competitive advantage
- Dilution of brand, reputation and image.

In addition to the consequences to an organisation, others also suffer. Individuals whose data has been compromised may spend a lot of time, money and stress in recovering from identity theft or the correction of erroneous data – if they can discover which organisation(s) hold personal data about them. Some people may be put at risk if their privacy or personal data is compromised (e.g., undercover agents, celebrities, vulnerable populations, such as children and victims of domestic violence) or, for example, may face higher insurance premiums or difficulties in getting or retaining a job.

Even other companies who were not involved in an incident may suffer spillover effects, as Culnan and Williams point out in the ChoicePoint and TJX cases:

> Incidents experienced by a single firm can cause spillover effects with repercussions affecting an entire industry. . . . For example, the ChoicePoint breach motivated Congress to hold hearings to investigate information practices in the data broker industry. Following the TJX breach, Massachusetts issued its 2008 security rule, which imposes stringent organizational and technical requirements on anyone who maintains personal information on Massachusetts residents, with other states expected to follow (Smedinghoff and Hamady 2008). Legislation was also introduced in several states to hold all retailers responsible for the costs incurred by banks in reissuing new credit cards to individuals whose credit card numbers had been stolen in a breach (Bureau of National Affairs 2007b). Spillover effects such as new regulations can also threaten an organization's legitimacy because they can cause other firms in the same industry to incur substantial new costs even though they were uninvolved in the original crisis.[44]

The risk assessment and management process in many of its phases is a qualitative process, meaning that it involves a lot of subjective estimations; it is also flexible and provides many levels of granularity, in accordance with the assessment needs. It provides a solid methodological structure upon which a PIA can be based.

---

[42] Lipton, Eric, "Bowing to Critics, U.S. to Alter Design of Electronic Passports", *The New York Times*, 27 April 2005. http://www.nytimes.com/2005/04/27/politics/27passport.html?scp=11&sq=biometric+passport&st=nyt

[43] Peev, Gerri, "Labour in Retreat as ID Card Plan is Axed", *The Scotsman*, 1 July 2009. http://thescotsman.scotsman.com/uk/Labour-in-retreat-as-.5415982.jp

[44] Culnan and Williams, op. cit., p. 683.

1.4.2 To Derive Benefits

A company or government department that undertakes a PIA with good intent, with a genuine interest in engaging stakeholders, including the public, has an opportunity of earning trust and goodwill from citizen-consumers. The extent to which it earns trust and goodwill will be a function of how open and transparent the organisation makes the PIA process. The more open and transparent the process is, the more likely the organisation is to overcome apprehensions, suspicions and mistrust in the development of a new service, product, policy, programme or project.[45] Even if a new service does not engender public concerns (or those of privacy advocates), and there appears to be no mistrust to overcome, the organisation can earn goodwill for being open and transparent about what it is planning to do. Businesses able to sustain a high level of trust and confidence can differentiate themselves from their rivals and thereby gain a competitive advantage.[46]

By engaging stakeholders in the PIA process, an organisation can benefit from ideas it may not have previously considered or it may find that stakeholders place much greater weight on some issues that the organisation had regarded as relatively minor. If the project does raise difficult issues with regard to privacy, ideas from stakeholders may be particularly welcome. Even if stakeholders don't manage to generate some new considerations, the organisation at least has an opportunity of gaining stakeholders' understanding and respect.

Transparency in the process may also be a way of avoiding liabilities downstream. If the organisation is able to demonstrate that it did engage and consult with a wide range of stakeholders, was forthcoming with information, considered different points of view, it will be more difficult for some stakeholders to claim subsequently that the organisation was negligent in its undertaking.[47] By being open and transparent from the outset, the organisation can minimise the risk of negative media attention.

The New Zealand PIA Handbook describes a privacy impact assessment as an "early warning system". The PIA radar screen will enable an organisation to spot a privacy problem and take effective counter-measures before that problem strikes the business as a privacy crisis. It goes on to say that the PIA process can help the organisation by providing credible information upon which business decisions can

---

[45] A PIA "enables an organisation to understand the perspectives of other stakeholders and make the aims of the project better understood." ICO, *PIA Handbook*, op. cit., p. 6. The Handbook seems to adopt the position of the project manager, rather than the privacy advocates, when it adds: "By actively seeking out and engaging the concerns of stakeholders, even those who are expected to oppose a particular project, you can discover the reasoning behind their position and identify where further information needs to be provided and pre-empt any possible misinformation campaigns by opponents of the project."

[46] Stewart, *PIA Handbook*, op. cit., p. 29.

[47] "A PIA provides an organisation with an opportunity to obtain a commitment from stakeholder representatives and advocates to support the project from an early stage, in order to avoid the emergence of opposition at a late and expensive stage in the design process." ICO, *PIA Handbook*, op. cit., p. 6.

be based and by enabling organisations to identify and deal with their own problems internally and proactively rather than awaiting customer complaints, external intervention or a bad press.[48]

As mentioned above, PIA is a form of risk assessment, an integral part of risk management. It encourages cost-effective solutions, since it is more cost-effective and efficient to build "privacy by design" into projects, policies, technologies and other such initiatives at the design phase than attempt a more costly retrofit after a technology is deployed or a policy promulgated. Some simple adjustments may be all it takes to make the difference between a project that is privacy intrusive and one that has built in necessary safeguards. Thus, a PIA creates an opportunity for organisations to anticipate and address the likely impacts of new initiatives, to foresee problems and identify what needs to be done to design in features that minimise any impact on privacy and/or to find less privacy-intrusive alternatives.

A PIA should also be regarded as a learning experience, for both the organisation that undertakes the PIA as well as the stakeholders who are engaged in the process. An open PIA process helps the public understand what information the organisation is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored.[49] The PIA's educational role is a way of demonstrating that the organisation has critically analysed how the project will deal with personal data. It might be the case that certain identified risks on privacy cannot be mitigated and/or have to be accepted (residual risks); even so, the PIA report, as the result of a clear and systematic process, is something to which interested parties can refer and be informed of the reasons why some assumptions were made decisions and decisions taken. Thus, a PIA promotes a more fully informed decision-making process.[50]

PIA can be used to enforce or encourage accountability. A PIA should make clear who intends to do what and who will be responsible for what. It should make clear that, as a minimum, the project is fully compliant with privacy laws, regulations and relevant codes of conduct. If an executive knows she will be held accountable for a privacy-intrusive action, she may be less inclined to proceed with an action that seems likely to anger the public or, if not the general public, at least privacy advocates or other stakeholders likely to contest the action in the media.

1.5 Variations in PIA Approaches

Just as the definitions of a privacy impact assessment vary, so too do the PIA methodologies. While there are similarities in approach, there are also differences, as indicated by Table 1.2, which is based on a comparison of the principal PIA

[48] Stewart, *PIA Handbook*, op. cit., pp. 6, 11.

[49] DHS, *PIAs: The Privacy Office Official Guidance*, op. cit., p. 4.

[50] Karol, Thomas J., *A Guide To Cross-Border Privacy Impact Assessments*, Deloitte & Touche, 2001. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/A-Guide-To-Cross-Border-Privacy-Impact-Assessments.aspx

Table 1.2 Similarities and differences in national PIA methodologies

PIA features	Australia	Canada	NZ	UK	US
PIA is mandated by law or must accompany budget submissions.		✓	V	✓	✓

In this table, V = variations. Principally these variations refer to differences in approaches to PIA among different Executive branch agencies in the US government

guidance documents at national level in Australia, Canada, New Zealand, the United Kingdom and the United States.

Of the five countries, the US is virtually unique in having legislation that mandates PIA. Section 208 of the E-Government Act of 2002 requires all Executive branch departments and agencies to conduct a PIA for all new or substantially changed systems that collect, maintain or disseminate personally identifiable information (PII). New Zealand's Immigration Act 2009 makes PIAs mandatory for systems collecting and "handling" biometric data (see Chapter 8). The Treasury Board of Canada requires federal departments and agencies to submit a PIA with funding submissions.[51] The UK government has made PIAs obligatory for government agencies,[52] but as there is no reporting requirement, or enforcement mechanism, it is impossible to know whether government departments and agencies are, in fact, carrying out PIAs.

PIA features	Australia	Canada	NZ	UK	US
PIA guidance is targeted at government departments and agencies only.		✓			✓

The US OMB guidance, while focused on Executive departments and agencies, does say that government contractors are also obliged to perform a PIA for IT projects that process PII.

[51] "Federal organizations seeking preliminary project approval (PPA) from the Treasury Board pursuant to the Project Management Policy must include the results of the Privacy Impact Assessment (PIA) in the body of the submission or project brief, where applicable." Treasury Board of Canada Secretariat, "A Guide to Preparing Treasury Board Submissions", Annex D, section 4. http://www.tbs-sct.gc.ca/pubs_pol/opepubs/TBM_162/gptbs-gppct09-eng.asp#d4. See also the TBS Privacy Impact Assessment Policy, section on accountability, 2 May 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text

[52] The Cabinet Office has stated that the government has accepted the value of PIAs and that they will be used in all departments. UK Cabinet Office, Data Handling Procedures in Government: Final Report, London, June 2008, para 2.11. http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

PIA features	Australia	Canada	NZ	UK	US
PIA guidance is targeted at government departments *and* the private sector.	✓	V	✓	✓	

In Canada, while the Treasury Board PIA guidelines have been prepared for government departments and agencies, PIA guidance at the provincial level is targeted at the private sector as well.

PIA features	Australia	Canada	NZ	UK	US
PIA guidance has been prepared by the funding agency.		✓			✓

The key PIA guidance document in Canada is that prepared by the Treasury Board Secretariat. In the US, it is that by the Office of Management and Budget. However, various US departments and agencies have prepared PIA guidance documents. The DHS guide is particularly good and somewhat more detailed than that of the OMB.

PIA features	Australia	Canada	NZ	UK	US
PIA guidance has been prepared by the privacy commissioner.	✓		✓	✓	
PIA should be initiated at early stage of project development, before decisions are taken.	✓	✓	✓	✓	✓
PIA guidance identifies benefits of undertaking a PIA.	✓	✓	✓	✓	✓
A PIA is regarded as a form of risk management.	✓	✓	✓	✓	✓
PIA guidance focuses on privacy risks involving personally identifiable information (aka informational privacy).	✓	✓	✓	✓	✓

PIAs are generally concerned with informational privacy. However, they could also address other types of privacy, something explicitly not ruled out by the Australian Guide[53] or the UK PIA Handbook.[54] The DHS Guidance seems to agree, at least implicitly, when it says, "A body screening device may capture the full

[53] "Information privacy is only one aspect of privacy. Other types of privacy include bodily privacy, territorial privacy, and communications privacy. These can be considered in the PIA process, particularly where they may pose risks to the overall success of the project." [Australia] OPC, *PIA Guide*, op. cit., p. iii.

[54] ICO, *PIA Handbook*, op. cit., pp. 6, 14, 85.

scan of an individual. While the information may not be maintained for later use, the initial scan may raise privacy concerns and a PIA could be required. Examples of technology with privacy implications could include: systems utilising radio frequency identification devices (RFID), biometric scans, data mining, or geospatial tracking."[55]

PIA features	Australia	Canada	NZ	UK	US
PIA guidance envisages a PIA as a multi-disciplinary exercise.	✓	✓			✓

The OMB guidance sees collaboration by different stakeholders, although it does not specifically say stakeholders external to the agency: "To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy." The Treasury Board of Canada Secretariat's PIA policy says PIAs "are co-operative endeavours requiring a variety of skill sets, including those of program managers, technical specialists and privacy and legal advisors." The Australian PIA Guide similarly says: "a PIA generally means a team approach. It makes use of the various 'in-house experts'. . . and outside expertise as necessary."

PIA features	Australia	Canada	NZ	UK	US
PIA guidance puts emphasis on PIA as a process and not just preparation of the PIA report.	✓	✓		✓	

But reports are important too, as the DHS has said: "By documenting the procedures and measures through which the Department protects the privacy of individuals, the Department is more transparent and can better carry out its mission." Even the UK's ICO, which places heavy emphasis on PIA as a process, does not dismiss the importance of a PIA report:

The reasons for preparation of a PIA report are:

- as an element of accountability, in order to demonstrate that the PIA process was performed appropriately;
- to provide a basis for post-implementation review;
- to provide a basis for audit;
- to provide corporate memory, ensuring that the experience gained during the project is available to those completing new PIAs if original staff have left; and
- to enable the experience gained during the project to be shared with future PIA teams and others outside the organisation.[56]

[55] DHS, *PIAs: The Privacy Office Official Guidance*, op. cit., p. 5.

[56] ICO, *PIA Handbook*, op. cit., p. 39.

PIA features	Australia	Canada	NZ	UK	US
PIA guidance explicitly encourages engaging external stakeholders in the PIA process.	✓	V	✓	✓	

Canadian PIA policy does not explicitly say that stakeholders should be engaged in undertaking a PIA, but the PIA Guidelines say that a PIA can be "the basis for consultations with stakeholders", and in its checklist of questions, there are two that ask if key stakeholders have been provided with an opportunity to comment on the privacy protection implications of the proposal and whether public consultation will take place on the privacy implications of the proposal.

Generally, with the notable exception of the Canadian PIA Guidelines and the UK Handbook, PIA guidance documents do not describe in any detail PIA processes and, especially, stakeholder consultation mechanisms and participatory deliberation. Ortwin Renn has observed that "the European Union has highlighted the need for more stakeholder involvement and participation in risk management. However, how to implement this in day-to-day risk management is still under dispute."[57] His comment applies equally to PIA.

PIA features	Australia	Canada	NZ	UK	US
The PIA guidance contains a set of privacy principles.	✓	✓	✓	✓	V

The DHS PIA Guidance contains the Fair Information Practice Principles (FIPPs). The OMB Guidance does not. The Canadian PIA guidelines are based on privacy principles in the Code of Fair Information Practices in the federal Privacy Act as well as the 10 privacy principles attached to the Personal Information Protection and Electronic Documents Act (PIPEDA).

PIA features	Australia	Canada	NZ	UK	US
The PIA guidance puts primary emphasis on compliance.					V

All PIA guidance documents mention the importance of compliance with laws, regulations and/or codes of practice, but while compliance is important, it is not necessarily the primary purpose of the PIA. (The primary purpose is to identify risks to privacy and ways of dealing with those risks.)

[57] Renn, op. cit., p. 81. He cites European Commission, European Governance: A White Paper, COM (2001) 428 final, Brussels, 2001.

PIA features	Australia	Canada	NZ	UK	US
The PIA guidance provides questions for consideration during the PIA process or in preparing a PIA report.	✓	✓	✓	✓	V

The DHS Guidance contains a set of questions (unlike the OMB Guidance). While checklists can be criticised as mere box-ticking exercises, the questions usually require more than a straight yes or no response, i.e., the assessor or project manager is expected to describe the "how" or "what". In any event, the long lists of questions are actually valuable in prompting consideration of issues that might otherwise be neglected.

PIA features	Australia	Canada	NZ	UK	US
The PIA guidance contains a template for preparation of the PIA report.	✓	✓	✓	✓	V
PIAs are scalable, i.e., no one size fits all.	✓			✓	✓

"Because organisations vary greatly in size, the extent to which their activities intrude on privacy, and their experience in dealing with privacy issues makes it difficult to write a 'one size fits all' guide", says the UK Information Commissioner's Office.[58] "The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system", as the OMB guidance puts it. The UK Handbook offers templates for a "small-scale" PIA and a "full-scale" PIA. The Canadian PIA policy distinguishes between a "preliminary" and a "comprehensive" assessment.

PIA features	Australia	Canada	NZ	UK	US
The PIA policy provides for third-party, independent review or audit of the completed PIA document.		✓			V

According to the Canadian Directive on PIA,[59] government institutions must ensure "the approved core PIA provided to TBS is simultaneously provided to the Office of the Privacy Commissioner". Further, "heads of government institutions are required to notify the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the Privacy Act or to any of its

[58] ICO, *PIA Handbook*, op. cit., p. 2.

[59] Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment, Ottawa, 1 April 2010. This directive replaces the Privacy Impact Assessment Policy of 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text

provisions or that could have an impact on the privacy of Canadians. This notification is to take place at a sufficiently early stage to permit the Commissioner to review and discuss the issues involved." The US Government Accountability Office (GAO), which bills itself as "the investigative arm of Congress", reviews PIAs prepared by Executive branch departments and agencies.

PIA features	Australia	Canada	NZ	UK	US
The PIA report and/or summary is to be published on the agency's website.		✓	V		✓

The Australian PIA Guide advocates (p. x) publishing the contents and findings of a PIA, but does not require it. The New Zealand PIA Handbook also advocates (p. 19) publishing the PIA findings, but does not require it. However, the NZ Immigration Act 2009 does require that PIAs regarding the collection and processing of biometric data be published on the department's website (see again Chapter 8 of this book). When the author asked for a PIA from a UK government department, he was told it would require a Freedom of Information request.

PIA features	Australia	Canada	NZ	UK	US
The PIA guidance says the PIA report may need to be revised and updated or a new PIA process undertaken.	✓	✓	✓	✓	✓

The DHS PIA guidance says, "The PIA is a living document that needs to be updated regularly as the program and system are changed and updated, not just when the program or system is deployed."[60] The New Zealand PIA Handbook also regards a PIA as a kind of "living" document.[61] And the Canadian PIA guidelines say, "A PIA is a dynamic process and as design changes occur in the business processes, the PIA should also be reviewed and updated."

1.6 Open Issues

As shown above, there are differences in the national approaches to PIA. Each has some good points as well as some shortcomings. Some of these shortcomings concern "open issues" discussed in this section as well as in subsequent chapters in this

[60] DHS, *PIAs: The Privacy Office Official Guidance*, op. cit., p. 2.

[61] "The privacy impact report can be an evolving document which will become more detailed over time." Stewart, *PIA Handbook*, op. cit., p. 17.

book. By "open issues", we mean issues that have been or are subject to debate, but on which as yet there has been no consensus, no general agreement on a common approach.

1.6.1 Scale and Scope of the PIA

The Australian guide says the first question to ask when assessing whether a PIA is needed is: "Will any personal information be collected, used or disclosed in the project?"[62] This is known as a threshold assessment. If the answer is yes, then a PIA is needed.

The scale and scope of a PIA depend on the significance of the project, the extent to which it collects, uses or discloses personal information, the PIA budget, the time it takes to conduct the PIA and the PIA's terms of reference. The Australia guide comments (p. xxv), "The more significant the scope, the more comprehensive the PIA should be." Conversely, if a project is relatively limited in scope, only a short PIA may be needed. Nevertheless, the guide advises (p. xxvi) that even a shorter PIA should address all of the key stages. Other PIAs may also be necessarily short, for example, "projects at the conceptual stages of development may only be able to address the PIA key stages in a less-detailed way" (p. xxvi). As the project develops and the issues become clearer, the PIA can be updated and supplemented, becoming more comprehensive. Others, such as the UK Handbook, have adopted a similar approach. The UK distinguishes between small-scale and full-scale PIAs.

Although the Australian PIA Guide deals with informational privacy, it notes (p. xx) that the PIA methodology could also be used for other types of privacy, such as bodily, territorial or communications privacy. The UK PIA Handbook similarly, but perhaps more explicitly, says (p. 14) a PIA could consider privacy of personal information, of the person, of personal behaviour and of personal communications. They are among the few PIA guides that make this distinction.

Most guidance documents give considerable discretion to organisations to determine (a) whether a PIA is needed and (b) the scale and scope of the PIA. Even in the US where the OMB obliges Executive branch departments and agencies and their contractors to undertake a PIA if they process personal data, and where they are obliged to report annually on their use of PIA, some PIAs can only be described as perfunctory at best, as short as two pages (see Chapter 10 by Kenneth Bamberger and Deirdre Mulligan).

There is little information available about the cost of a PIA. The cost will, of course, depend on the scale of the PIA, including the extent to which the project manager consults and engages with stakeholders, on the budget allocated for undertaking a PIA. To ask how much an "average" PIA costs is like asking "How long is a piece of string?". An equally critical consideration is how long it might take to perform the PIA. There may be considerable pressure, especially in the private

[62] OPC, *PIA Guide*, op. cit., p. xi.

sector, to complete a project, to develop and commercialise a service or to get a new technology or product into the market, with corresponding pressure to complete a PIA quickly so as not to delay the project.

Another related issue of importance is the terms of reference of the PIA team. The UK PIA Handbook, uniquely among the PIA guidance documents, discusses the terms of reference of the PIA team:

It is generally advisable for terms of reference for the PIA to be prepared and agreed. Important elements of the terms of reference include:

- the functions to be performed;
- the deliverables;
- the desired outcomes;
- the scope of the assessment; and
- the roles and responsibilities of various parties involved in the PIA.

The terms of reference should document the governance structure and processes, including the nature of the delegation of responsibility and authority provided to the person(s) or team(s) who are involved in the PIA.[63]

1.6.2 Who Should Perform the PIA?

In the first instance, the project manager (or policy-maker or technology developer) should be responsible (and accountable) for deciding whether a PIA should be carried out, the scale and scope of the PIA, and who to involve in undertaking the PIA. The Australian Guide says (p. ix), "Generally, whoever is handling the project is responsible for deciding if a PIA is necessary or desirable and ensuring it is carried out." Some projects will have markedly more privacy impact than others, in which case a "robust and independent PIA conducted by external assessors may be preferable". An "independent assessment may also help the organisation to develop community trust in the PIA findings and the project's intent" (Australian Guide, p. x).

PIAs may be prepared "in-house" or by consultants. Each has advantages. The New Zealand PIA Handbook says (p. 5) that "There are distinct advantages in outsourcing the preparation of a privacy impact report to lend impartiality to the process. That may be critical in influencing consumer or public opinion. Nonetheless, it is feasible to undertake PIA in-house, using the skills and experience of the project team and the wider organisation." Elsewhere, it says (p. 13), "Sometimes most of the necessary skills will reside in the team assembled to develop the project itself. Experts with particular skills may be brought in to assist with certain aspects. An agency's Privacy Officer may undertake a coordinating or checking role."

The PIA may also be undertaken by a mix of people, some in-house personnel, some external to the organisation. The NZ PIA Handbook says (p. 14), "Competent

[63] ICO, *PIA Handbook*, op. cit., p. 10.

privacy expertise. . . may be brought in even when most of the work will be done by the project team. . . . Where the PIA is solely undertaken internally, thought should be given to incorporating some external or independent oversight. One possibility is to use a privacy or data protection consultant to carry out such a check."

1.6.3 Should Engaging External Stakeholders Be Part of the PIA Process?

Some organisations may not want to engage external stakeholders in the performance of a PIA. They may feel the complexity of the project is such that it would take a big effort to "educate" or bring up to speed the external stakeholders to the point where they may be able to provide meaningful insights. They may not want to engage external stakeholders because they assume consensus would be too difficult to achieve given the diversity of opinion about the project. Or they may not want to deal with the criticism they may get. Or they may feel the project is too commercially sensitive or involves national security. Such considerations will usually be short-sighted. There are ways of responding to such objections, as Raab and Wright point out in Chapter 17.

The value of engaging with stakeholders is worth the effort. Australia's PIA Guide says (p. x), "Consultation with key stakeholders is basic to the PIA process." It adds that

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

Engaging stakeholders in the PIA process has many benefits to the organisation. The benefits identified by the ISO in its standard on information security risk management are equally applicable to a PIA. Engaging stakeholders can help an organisation to

- Identify risks that might not otherwise be considered[64];
- Communicate the results of the organisation's risk assessment and how it intends to deal with those risks;

[64] ICO is of the view that if a PIA is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It therefore recommends that stakeholder perspectives are considered. See ICO, *PIA Handbook*, op. cit., p. 56. At p. 58, it makes the precision that risks may be overlooked unless they are considered from the various perspectives of each of the stakeholder groups, rather than just from the viewpoint of the organisation that is conducting the project. "There are often different impacts and implications for different sections of the population, especially disadvantaged groups."

- Avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision-makers and stakeholders;
- Support decision-making;
- Co-ordinate with other parties and plan responses to reduce the consequences of any incident;
- Give decision makers and stakeholders a sense of responsibility about risks;
- Improve awareness.[65]

1.6.4 Should PIAs Be Published?

The US E-Government Act of 2002 obliges the publication of PIAs. The US Department of Homeland Security publishes "approved PIAs" on its Privacy Impact Assessment web page[66] unless they are classified.

The Treasury Board Secretariat of Canada says only summaries of PIAs need publication on a government department or agency's website.

While others don't require publication, they advocate it. For example, the Australian PIA Guide (p. x) advocates publishing the contents and findings of a PIA because it "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". However, the Australian Privacy Commissioner has acknowledged (p. xviii) that "there may be circumstances where the full or part release of a PIA may not be appropriate. For example . . . there may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part." Where there are difficulties in making the full PIA available, the Commissioner encourages release of a summary version.

The New Zealand PIA Handbook advocates (p. 19) publishing the PIA findings: "Usually, there is merit in making completed privacy impact reports publicly available and organisations should consider posting the privacy impact report or a summary on their website. Openness about the findings can contribute to the maintenance of public trust and confidence in the organisation and can ensure that its practices and policies in relation to the handling of personal information are fair and freely available."

The ICO seems to favour publication as well,[67] but it is not mandatory, nor is there any reporting mechanism in the UK, so it is virtually impossible to know whether a PIA has been performed unless an organisation chooses to say so, and it would appear that few do so.

---

[65] ISO/IEC 27005:2008(E), op. cit., p. 22.

[66] http://www.dhs.gov/files/publications/editorial_0511.shtm

[67] ICO, *PIA Handbook*, op. cit., pp. 39, 40.

While some organisations, for competitive or security reasons, may not want to publish a PIA, the sensitive information can be redacted or separated into an appendix, which can be distributed less widely and/ or subject to confidentiality constraints.

1.6.5 Should PIAs Be Mandatory?

It could be argued that in view of the many instances when personal data has been compromised, PIAs should be mandatory.[68] The European Commission, in its Communication of 4 November 2010, seems to suggest that, in its envisaged revision of the Data Protection Directive, any data controller processing sensitive personal information would be obliged to conduct a PIA.

Not all PIA advocates favour making PIAs mandatory. For example, some argue that making PIAs mandatory reinforces "a 'compliance mentality' view of the PIA as yet another hurdle to be overcome in the already cumbersome project and funding process".[69]

There are practical difficulties in making PIAs mandatory. One difficulty is in determining when a PIA should be conducted. As the Australian PIA Guide (p. xx) says, "There is no hard-and-fast rule about when to do a PIA, and each project must be considered individually." A second difficulty is in determining the scale and scope of a PIA. If there were a directive or regulation that made PIAs mandatory, how would the parameters be drawn as to what constituted a PIA? Making PIAs mandatory might lead to some companies conducting the most cursory of PIA, a simple, one-page box-ticking exercise. It would be difficult to enforce a mandatory requirement. Would we need a PIA police force?

While there are difficulties, it is also possible to envisage solutions to some of these difficulties. For example, for government agencies, PIAs could be tied to funding submissions. If the funding agency (e.g., the Treasury Board of Canada) did not find the PIA of acceptable quality, it could withhold funding until the PIA was deemed acceptable. Requiring the deputy minister to sign off the PIA would bring accountability to bear. In the case of a company in the private sector, PIAs could be deemed to be part of good risk management practice. The company would be obliged to state how it is managing risks, including risks to privacy, in its annual report. PIAs could be made subject to independent, third-party review or audit.

---

[68] Wright, David, "Should Privacy Impact Assessment Be Mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121–131.

[69] Hope-Tindall, Peter, "Privacy Impact Assessment – Obligation or Opportunity: The Choice is Ours!", *Prepared for CSE ITS Conference*, Ottawa, ON, 16 May 2002. http://www.home.inter.net/gt/grabbag/Tindall_PIA_Material.pdf

1.6.6 Should the DPA or Privacy Commissioner "Approve" a PIA?

The Alberta Office of the Information and Privacy Commissioner will not "approve" a PIA submitted to them by an organisation. Once satisfied that the organisation has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner will "accept" the PIA. Acceptance is not approval; it merely reflects the Commissioner's acceptance that the organisation has made reasonable efforts to protect privacy.[70]

In the instance of the Canadian federal government, departments and agencies are required to copy the Office of the Privacy Commissioner on the PIAs sent to the Treasury Board for funding submission.[71] In the UK, while PIAs are supposedly obligatory for government departments, there is no obligation for the Information Commissioner's Office to be sent a copy of the PIA,[72] nor are PIAs tied to funding submissions, so it would appear impossible to know whether government departments are, in fact, producing PIAs or how rigorous those PIAs might be.

The difficulty facing many data protection authorities and privacy commissioners is that they do not have the resource to review, let alone approve PIAs. Their review and approval of PIAs produced in the private sector would be an even more remote possibility.

Nevertheless, one could envisage solutions to this problem. One is to make PIAs subject to independent, third-party audit, much like financial accounts of companies listed on the stock exchange. Another is to require publication of the PIA (with legitimate exceptions or redacted as necessary in cases involving crime prevention or national security). Yet another is to create a national registry of PIAs, at least of those performed by government departments and agencies, which would make it easier for researchers, privacy advocates and others to find those relevant to their interest. Copying PIAs to the privacy commissioner seems like a good idea; even if the privacy commissioner is not able to review each one, it could review or carry out a random audit of at least some of them. Unless a PIA policy has some teeth, PIAs are unlikely to live up to expectations, as Nigel Waters (see Chapter 6) and others in this book have observed.

---

[70] http://www.oipc.ab.ca/pages/PIAs/Description.aspx

[71] "Government institutions must provide a copy of the final Privacy Impact Assessment to the Privacy Commissioner. This notification must occur at a reasonably early stage prior to implementing the initiative, program or service. Advance notification is intended to permit the Commissioner to review the issues and, if appropriate, to provide advice to the head of the institution." TBS, "Privacy Impact Assessment Policy", op. cit.

[72] In fact, the ICO PIA Handbook explicitly says (p. 11): "PIAs have been designed as a self-assessment tool for organisations and the ICO does not have a formal role in conducting them, approving or signing off any final report which is produced."

1.6.7 Should a PIA Apply to the Development of New Policy?

Canada's Directive on PIA says it "does not apply to the development of new legislation".[73] Although the policy says a PIA is to be applied for new programs or services, the PIA Guidelines say "A PIA is a process that helps departments and agencies determine whether new technologies, information systems and initiatives or proposed programs *and policies* meet basic privacy requirements." [Italics added.]

The ICO PIA Handbook says that a PIA could apply to "a system, database, program, application, service or a scheme, or an enhancement to any of the above, or an initiative, proposal or a review, *or even draft legislation*."[74] [Italics added.]

1.6.8 Two or More Organisations Collaborating on a PIA

Although Canada's PIA policy applies to both intra- and inter-departmental initiatives,[75] generally PIA policy and practice have focused on the individual organisation conducting a PIA, so there is the distinct possibility that projects, policies, systems, programs or technologies involving the collection and processing of personally identifiable information by two or more organisations escape the attention of a PIA. The audit undertaken by the Office of the Privacy Commissioner (see Chapter 20 by Jennifer Stoddart) has drawn attention to this fact. Hence, there would appear to be a requirement that PIA policy should cast its net more widely to ensure that projects involving two or more organisations are caught within its purview. There may be some logistical hurdles to be overcome in undertaking such PIAs, such as who would be responsible for leading the PIA and who would be held accountable for its adequacy, but these need not be insurmountable. If the organisations could not come to some agreement on such issues, the privacy commissioner could arbitrate or, if not the privacy commissioner, then the funding agency (e.g., the OMB in the US or the Treasury Board in Canada or the Cabinet Office in the UK). An alternative to a single PIA involving two or more organisations is two or more PIAs, each carried out by each organisation involved in the project.[76] A potential downside for such an approach is that the different PIAs come to different conclusions with regard to the privacy risks and how they should be mitigated. It would be desirable for government departments and agencies to come to some arrangement in such cases, so they could be cited as good practice to companies who similarly collaborate on projects. The European Commission and government procurement

---

[73] TBS, Directive on Privacy Impact Assessment, op. cit., section 2.4.

[74] ICO, *PIA Handbook*, op. cit., p. 2.

[75] And the Canadian PIA Guidelines contain a questionnaire designed for cross-jurisdictional initiatives.

[76] This is the approach recommended in the Canadian TBS PIA Guidelines: "An operating assumption for the development of the cross-jurisdictional PIA is that individual jurisdictions should complete their own PIA based on their specific statutory and policy provisions."

agencies could play a helpful role here too, e.g., when they elicit proposals from consortia for projects involving the collection and processing of personal data, they could specify a requirement for a PIA and it would be up to the consortium to decide on the practical procedures for its conduct (i.e., who would be responsible and accountable).

1.6.9 Are Trans-national PIAs Feasible?

So far, there have been almost no instances of a trans-national PIA, yet there are many projects or programmes that involve the participation of two or more countries, notably in regard to law enforcement and financial transactions in pursuit of criminals and terrorists. Such international projects or programmes often involve personal data and, with minimal oversight, the risk of unwarranted or disproportionate privacy intrusion appears to be particularly high. The hurdles mentioned above would appear to be even higher where national sovereignty is involved.

While there have been almost no instances of a trans-national PIA, some groundbreaking has taken place. Charles Raab and David Wright mention in Chapter 17 the case of a trans-national PIA involving medical data as well as the PIA guide prepared in 2001 by Deloitte and Touche specifically devoted to cross-border privacy impact assessment. Raab and Wright also suggest ways forward for the conduct of trans-national PIAs. Artemi Rallo, Director of Spain's Data Protection Agency, discusses the prospects for trans-national PIAs in Chapter 18.

1.7 Objectives and Scope of This Book

This book has three main objectives. First is to provide a reasonably comprehensive overview of PIA activity around the world. Second is to identify open issues, where there are differences of views or where no common approach has yet been achieved with regard to PIA policy and practice. Third is to identify some of the best elements of existing PIA policy and practice in order to make recommendations to policymakers, industry and other stakeholders on how PIA practice can be improved.

The book is divided into several parts. Following the Foreword by Gary Marx, the first part includes this Introduction, Chapter 2 on a human rights perspective on privacy and data protection impact assessments, Chapter 3 on regulatory impact assessment and what lessons can be learned for PIA, and Chapter 4 on prior checking, a forerunner to privacy impact assessments.

The second part covers PIA practice in Australia, Canada, New Zealand, the United Kingdom and the United States, the five countries with the most experience of PIA.

The third part includes chapters from Nokia, Siemens and Vodafone, three global companies, representatives from which describe their use of PIAs and how they assess privacy impacts in their organisations.

The fourth part covers two specialised PIAs, including that developed by and for the financial services industry under the auspices of the International Organization

for Standardization, as well as two chapters devoted to the RFID PIA framework developed by industry and approved by the Art. 29 Data Protection Working Party in the European Union.

The fifth part addresses some specific issues – surveillance, the Madrid Resolution and the prospects for transnational PIAs, privacy and ethical impact assessments, the Canadian experience in auditing PIAs, optimising the regulator's role and, finally, the concluding chapter where we highlight some of the key findings from the contributions to this book and where we make recommendations for improving PIA policy and practice.

We are fortunate in having so many distinguished experts represented in this book. They are among the leaders in the field and include some of the earliest proponents of PIA. The authors include privacy commissioners, representatives from industry, academics and consultants. They have a wealth of experience with privacy impact assessment, which they kindly share with readers of this book. We, the editors, are grateful indeed that they have been willing to contribute to our project.

As stated at the outset of this Introduction, there is growing interest in PIAs. We hope that the experience evidenced in this book will help shape PIA policy and practice among those countries and companies contemplating the use of PIA to protect privacy against an increasing number of incursions.