available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy impact assessment: Its origins and development

Roger Clarke[a,b]

[a]*Xamax Consultancy Pty Ltd, Canberra, Australia*
[b]*CLSR Editorial Board*

Keywords:
Privacy
Privacy strategy
Privacy impact
Privacy impact statement
Technology assessment
Data matching program protocol

ABSTRACT

Privacy impact assessment (PIA) is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme. Its use has become progressively more common from the mid-1990s onwards.

On the one hand, privacy oversight agencies and privacy advocates see PIAs as an antidote to the serious privacy-intrusiveness of business processes in the public and private sectors and the ravages of rapidly developing information technologies. On the other, governments and business enterprises alike have struggled to encourage public acceptance and adoption of technologies that are very apparently privacy-invasive, and have been turning to PIAs as a means of understanding concerns and mitigating business risks.

This paper distinguishes PIAs from other business processes, such as privacy issues analysis, privacy law compliance checking and privacy audit, and identifies key aspects of the development of PIA practice and policy from their beginnings through to the end of 2008.

1. Introduction

On Google Scholar, the highest citation-counts for articles on the topic of privacy impact assessment (PIA), as late as the third quarter of 2008, appeared to be 24, 17, 16, 9 and 9 (for Carter, 2000; Clarke, 1998a; Kenny and Borking, 2002; Raab, 2004; Flaherty, 2000 respectively). The ISI Web of Science catalogue, searching across titles only and within a much more restrictive set of journals, disclosed precisely two papers, neither with any citations.

The lack of interest in academic circles contrasts with the situation in the policy arena, where the topic has attracted considerable attention, the practice is established, and the method is well-documented. Considerable activity has been evident in the U.K. during 2008, following the publication of a PIA Handbook by the Information Commissioner's Office (ICO, 2007b). An overview of the project that gave rise to it appeared in CLSR 24, 3 (Warren et al., 2008).

PIAs are often conducted in a highly-charged environment, and the interests of groups with varying degrees of power are usually in at least apparent conflict, and are sometimes locked in combat in a zero-sum game. It is therefore important to document the origins and early history of the method, to inform the inevitable debates of the coming years.

This paper commences with a brief review of the privacy arena, to provide the context within which PIAs have emerged. A definition is provided, and key characteristics of the process described. The paper then identifies related notions that pre-date PIAs and on which the formulation of PIA processes could be based. Applications of 'impact assessment' thinking to privacy issues are identified which pre-date uses of the term PIA. The emergence of the related terms privacy impact 'statement' and 'assessment' are documented. Important threads in the development of PIAs in various countries are noted. In addition to literature relevant to the history of PIAs, references are provided to definitions, guidelines and exemplars.

2. Privacy

Privacy has become a major social issue only since the 1960s. Its emergence as a significant policy consideration can be

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2009.02.002

attributed to the enormous expansion of threats to it. These have arisen from a combination of the increased scale of social and economic institutions, the increasingly professional and mechanistic forms of management in both the private and public sectors, increasing information-dependence to cope with the reduction in face-to-face contact, and advances in information technology, all feeding off one another (Clarke, 1988. See also Flaherty, 1989; Bennett, 1992).

The 'fair information practices' (FIP) movement emerged from the late 1960s, partly in Europe, but particularly in the USA in the work of Westin (Westin, 1967, 1971; Westin and Baker, 1974). Its purpose was less to protect privacy than to respond to privacy concerns from the perspective of the organisations that were increasingly impacting on it. The FIP movement involved the establishment of bodies of principles that purported to provide protections against the impacts of business practices and technology, while having the minimum possible impact on business and government administration. The still-prevalent attitude in US business and government is well-expressed in this quotation: ''I think it quite likely that self-discipline on the part of the executive branch will provide an answer to virtually all of the legitimate complaints against excesses of information-gathering'' (Rehnquist, 1971, then a spokesperson for the US Justice Department, subsequently US Chief Justice, quoted in Rule et al., 1980, p. 147).

Of the various bodies of principles that were published during the 1970s, a few sought to impose substantial obligations on organisations (e.g. HEW, 1973; NSWPC, 1977; PPSC, 1977). Most, however, adopted the narrower and (for organisations) less painful formulations consistent with FIP. A key feature was the power of each organisation to define the purposes of its data processing systems. This has the effect that the collection, storage, use and disclosure principles enshrined in legislation and codes are built on sand, and hence provide only limited privacy protection. Another device was the establishment of weak privacy oversight agencies (variously Inspectorates, Registries and Commissions) with limited powers and limited resources.

The FIP movement achieved an international convention in the form of the OECD Guidelines (OECD, 1980). The Guidelines' pro-business and anti-privacy purpose was explicit and unequivocal: to ''… advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries'' (OECD, 1980). The OECD Guidelines have in turn shaped virtually all laws and guidelines since the end of the 1970s. New sets are still being produced, however, as business and government continue to seek relief from what they see as the more onerous among the impositions of the FIP/OECD model. Two of significance are the US Administration's 'safe harbor' provisions (USDOC, 2000) and the APEC Privacy Framework (APEC, 2005).

Although the nature of FIP was recognised by some commentators from the outset (e.g. Rule, 1974; Rule et al., 1980), it has only slowly permeated the consciousness of the wider public. Since 1980, with the exception of a few elements of the EU Directive (EU, 1995), there has been little further development in privacy protections. Existing laws still reflect both the pro-business-and-government/anti-privacy agenda of FIP, and the long-superseded information technologies of the 1970s. The scene during the closing years of the twentieth century included weak privacy oversight agencies, frustrated privacy advocacy organisations, and a public that was increasingly wary and evasive in its dealings with business and government. The conditions were ripe for a change in approach.

3. Privacy impact assessments

The concept of a PIA emerged and matured during the period 1995–2005. The driving force underlying its emergence is capable of two alternative interpretations. Firstly, demand for PIAs can be seen as a belated public reaction against the increasingly privacy-invasive actions of governments and corporations during the second half of the twentieth century. Increasing numbers of people want to know about organisations' activities, and want to exercise control over their excesses. Privacy oversight agencies call for the technique to be applied, and privacy advocacy organisations build them into their calls for action. From this perspective, the conduct of a PIA can be viewed as the ceding by large organisations of some of the substantial power that they exercise over citizens or consumers.

Alternatively, the adoption of PIAs can be seen as a natural development of rational management techniques. Many applications of information technology depend on their adoption by people, and compliance by people with the requirements of the resulting systems. Significant numbers of governmental and corporate schemes have suffered low adoption and poor compliance, and been subjected to harmful attacks by the media. Organisations have accordingly come to appreciate that privacy is now a strategic variable. They have therefore factored it into their risk assessment and risk-management frameworks. 'PIA' was the language talked by regulators and privacy lobbyists; so government in particular, and business to a lesser extent, have been increasingly adopting the term and the technique.

The meaning ascribed to the term 'PIA' has varied over time and across jurisdictions. Aspects are discussed progressively through this paper, and a collection of definitions is provided in Appendix 1. The interpretation adopted by the author is that a PIA is properly distinguished from other kinds of activities by the following characteristics:

- *a PIA is performed on a project or initiative* (i.e. a PIA is distinct from an organisational privacy strategy);
- *a PIA is anticipatory in nature,* conducted in advance of or in parallel with the development of an initiative, rather than retrospectively (i.e. a PIA is distinct from a privacy audit);
- *a PIA has broad scope in relation to the dimensions of privacy,* enabling consideration of privacy of the person, privacy of personal behaviour and privacy of personal communications, as well as privacy of personal data (i.e. a PIA is distinct from a mere 'data privacy impact assessment');
- *a PIA has broad scope in relation to the perspectives reflected in the process*, taking into account the interests not only of the sponsoring organisation, and of the sponsor's strategic partners, but also of the population segments affected by it,

at least through representatives and advocates (i.e. a PIA is distinct from an internal cost/benefit analysis or internal risk assessment);
- *a PIA has broad scope in relation to the expectations against which privacy impacts are compared*, including people's aspirations and needs, and public policy considerations, as well as legal requirements (i.e. a PIA is distinct from a compliance assessment, whether against privacy laws generally, or data privacy laws in particular, or a specific data protection statute);
- *a PIA is oriented towards the surfacing both of problems and of solutions to them* (i.e. a PIA is more than just a privacy issues analysis);
- *a PIA emphasises the assessment process* including information exchange, organisational learning, and design adaptation (i.e. a PIA is not merely focused on the expression of a carefully-worded privacy impact statement);
- *a PIA requires intellectual engagement from executives and senior managers* (i.e. a PIA is not a mere checklist ticked through by junior staff or lawyers).

The following sections trace the way in which this contemporary interpretation of PIAs came about.

4. The emergence of PIAs

This section adopts a chronological approach to the emergence of PIAs, via its precursors, the concept, and the term 'privacy impact statement', to the term 'privacy impact assessment'.

4.1. *Precursors*

There would appear to be two primary intellectual threads that gave rise to the concept and term 'PIA'.

One is the idea of '*technology assessment*', as practised in the Office of Technology Assessment (OTA) of the US Congress, 1972–1995, and in a range of European contexts. An early treatment of the Office's methods is in OTA (1977). See also Porter et al. (1980).

The other progenitor is the '*impact statement*'. Its early application was in the form of Environmental Impact Statements (EIS), which originated in the 'green' movements of the 1960s. The US implemented a requirement for an EIS for major projects in 1970, and few jurisdictions in economically advanced nations are without some kind of requirement. There have been great tensions in this area, however. EIS are costly, and inevitably involve considerable delay. There has accordingly been a great deal of lobbying by powerful corporations, and by development-oriented government agencies, resulting in a wide array of compromises to the processes and products.

Of even greater relevance to the history of PIAs has been the cynicism about the EIS notion that arose among the people affected by major projects. If the law only requires that an EIS be prepared, then there remain many ways in which projects can gain approval despite having excessive negative impacts on the environment. The process that produces the EIS may be subject to inadequate controls, insufficiently audited, or insufficiently auditable, and hence the EIS may succeed in glossing over problems. An EIS may gain insufficient media coverage, and hence a development-minded agency or government may be able to ignore illogic, and value negative impacts and negative public opinion very lightly.

A more substantial notion is '*impact assessment*' which is usefully defined as ''the identification of future consequences of a current or proposed action''. The weaknesses of an EIS are countered by the notion of an environmental impact assessment (EIA). This lifts the focus beyond product alone to include process, and is a more fully articulated concept, including prior publication, public consultation, further publication and review. Official training materials are provided by UNEP (2002). Many government agencies provide guidelines. EIS has become the document that is produced at the end of an EIA, rather than the end in itself.

A professional community exists, the International Association for Impact Assessment (IAIA), which has long since applied the idea beyond its environmental origins. In addition to guidance on environmental impact assessment (IAIA, 1999), IAIA also provides guidance on social impact assessment (IOCSIA, 1994; IAIA, 2003). See also the segment on social impact assessment in UNEP (2002) and Becker and Vanclay (2003).

Privacy is not a focal point of the social impact assessment movement, however. IAIA does not appear to have recognised PIA as a sub-domain, and its journal, after 25 volumes, does not appear to have published a single article on the topic.

4.2. *Origins of the concept*

The concept now widely referred to as a PIA did not arrive with a pre-determined name. Hence most of the early publications do not mention the term.

Data protection laws that pre-dated the OECD Guidelines (e.g. those of Hesse 1970, Sweden 1973 and Austria, Denmark, France and Norway all of which passed laws in 1978) commonly required registration or licensing, and a check was necessary to ensure that the data controller's behaviour was in compliance with the law. Flaherty (1989, p. 405) documents instances where *pre-decisional assessments* were occasionally used in some European countries such as the Scandinavian countries and the U.K., and Bygrave (2002) points out that the Norwegian Data Inspectorate was required to assess ''whether the establishment and use of the register in question may cause problems for the individual person …'' (s. 10, Norwegian Personal Data Registers Act of 1978, since superseded). Impact assessment involves a much broader study than merely compliance with a specific law; but interpretations and discretions within those laws would have doubtless enabled the privacy oversight agency to make some contributions along the lines of what would later be referred to as a PIA. See also Bennett (1992).

The process was institutionalised in 1995 in Article 20 of the European Directive, which mandated what is referred to as '*prior checking*' against applicable standards, particularly of sensitive information systems. This is further discussed in Section 5 below.

The concept is also evident in an important, early document on the other side of the Atlantic: ''*Each time a new*

personal data system is proposed (or expansion of an existing system is contemplated) *those responsible* for the activity the system will serve, as well as those specifically charged with designing and implementing the system, *should answer such questions as* … What purposes will be served by the system and the data to be collected? How might these purposes be accomplished without collecting these data? …'' (HEW, 1973, p. 51).

The final paragraph of Chapter 13 of a US Study Commission's report, PPSC (1977), states ''*Perhaps the most significant finding in the Commission's assessment of the [US] Privacy Act [1974]* arises from its examination of the vehicles available for evaluating and assessing existing record systems, new systems, and agency practices and procedures. *Quite simply, there is no vehicle for answering the question: ''Should a particular record-keeping policy, practice, or system exist at all?''* While the Act takes an important step in establishing a framework by which an individual may obtain and question the contents of his record, it does not purport to establish ethical standards or set limits to the collection or use of certain types of information. Without such standards, however, the principal threat of proliferating records systems is not addressed. Nowhere, other than in the ineffective section requiring the preparation and review of new system notices, does the Act address the question of who is to decide what and how information should be collected, and how it may be used. To deal with this situation, the Congress and the Executive Branch will have to take action'' (emphasis added in this paper).

It would therefore appear that the concept, although not yet the term, was in use in some quarters as early as the first half of the 1970s. Moreover, the notion was sufficiently well-developed for a national commission to frame one of its 160 recommendations around it (and indeed one that survived the endeavours of the Ford Administration to reduce the report's scope, although the recommendation was not taken up).

A later reference to a procedure readily recognisable as an antecedent to the PIA process appears in Australian legislation relating to the specific practice of data matching (referred to as 'computer matching' in the USA). The Data-Matching Program (Assistance and Tax) Act 1990 included in Schedule 1 a requirement for a '*program protocol*'. This is closely related to the PIA notion in that it includes requirements to document ''the justifications for the program, … what methods other than data matching were available and why they were rejected [and] any cost/benefit analysis or other measures of effectiveness which were taken into account in deciding to initiate the program'' (para. 3.1).

Another thread that contributes to the emergence of PIAs is *cost–benefit analysis (CBA)*. This is a cluster of techniques that enable the evaluation of a project based on narrow financial criteria, or on broader financial and non-financial factors, or on a yet broader range of factors in order to reflect perspectives additional to that of the sponsor. CBA was applied to the assessment of computer matching projects in Clarke (1995a). The proposal for a regulatory scheme for computer matching in Clarke (1995b) includes the equivalent of a PIA, although it does not use the term and it focuses more heavily on the scheme's benefits and costs than on its impacts and disbenefits.

4.3. *Origins of the term 'privacy impact statement'*

In keeping with usage in the precursor context of environmental impact, the original concept was of a 'statement' prepared as a condition precedent to approval of a project or to parliamentary debate about legislation. Flaherty has stated that he can document the use of the term as early as the 1970s (2000, footnote 3). However the first literature reference to the term 'privacy impact statement' located by this author is a passage published by Flaherty in 1989, quoting a 1984 document of the Canadian Justice Committee: ''The Justice Committee recommended … the submission of a privacy impact statement [by an agency to the Canadian Privacy Commissioner] in relevant situations. The Cabinet … rejects the formal requirement of an impact statement to accompany each piece of legislation [footnoted to Re Ternette and Solicitor General of Canada, Dominion Law Reports 10, 4th ser. (1984): 587]'' (Flaherty, 1989, p. 277–8, emphasis added in this paper).

Flaherty also uses the term at two other locations in the same book: ''The data protection agency can … [prepare] its own evaluations of the potential impact on personal privacy of proposed legislation and information systems. … It is important that small data protection agencies encourage the main government departments to prepare their own initial reviews of the impact of new technology, preferably in the form of 'privacy impact statements' …'' (Flaherty, 1989, p. 405, emphasis added in this paper); and ''The US Privacy Protection Study Commission wisely recommended the preparation of a privacy impact statements for each piece of federal legislation'' (p. 413, footnote 26, emphasis added in this paper). A search of PPSC (1977) does not detect any use of the term, although the concept (as discussed earlier) is indeed evident.

Several years later, also in Canada, and at the point in time when PIA began to become mainstream, a paper on smart cards by staff of the Ontario Information and Privacy Commissioner's office included a ''sample privacy impact statements'' (IPCO, 1993, emphasis added in this paper). It is unfortunately not part of the version of the document that is currently available on the Web.

4.4. *Origins of the term 'privacy impact assessment'*

The term that has been current since the mid-1990s is the more comprehensive 'PIA'. In addition to resulting in a less unattractive acronym, it has the effect of emphasising process rather than product, and encompasses published information, consultation, publication and review.

The earliest mention of the term that the author has identified is advice provided by Lance Hoffman (private communication, 2004) that he assisted in the preparation of a Berkeley, California ordinance requiring a Privacy Impact Assessment, and that the ordinance is included in Hoffman (1973). Some years later, Daniel et al. (1990) focused on privacy impacts of traffic management technologies (a predecessor term for what is currently referred to as Intelligent Transportation Systems), but referred to 'social impact assessment' rather than PIA. Stewart advised (private communication, 2004) that the term was used in Longworth (1992).

Early contributions were made by the then Ontario Privacy Commissioner Tom Wright (IPCO, 1993, 1994, 1995, 1997) and by the then British Columbia Privacy Commissioner David Flaherty (Flaherty, 1994, 1995). The earliest mention of the term for which the author can provide a copy is a document submitted to the Ontario legislature and entitled ''Pro-active Consideration of Access and Privacy Implications'' which recommended ''a regulation that requires institutions to conduct a privacy impact assessment, as defined in the regulation, prior to the introduction of any computer information systems'' IPCO, 1994, at s. 50, emphasis added in this paper).

By the mid-1990s, Privacy Commissioners and a small number of specialist consultants and academics, variously in Canada, New Zealand and Australia were thinking about PIAs in a systematic manner as an ''essential tool for data protection'' (Flaherty, 2000). The idea spread rapidly around the policy community, although, as will be discussed below, the formalisation of tools to implement the PIA process took a further 5–10 years to mature.

5. Articulation

Developments in PIA philosophy, law and practice occurred in parallel in various countries, and differed among them, in some respects substantially. Because this paper's focus is on the history of PIAs, it does not attempt a thorough intellectual examination, but merely identifies key aspects. It draws on a variety of sources, including ICO (2007a) and the detailed Appendices to that Study, C to I inclusive.

This section outlines developments in approximately chronological order, in the jurisdictions that, in the author's view, made the most significant contributions. The section is supported by Appendices that identify definitions, examplars and guidelines. The subsequent section identifies some key themes.

5.1. *New Zealand*

In 1996, Blair Stewart, Deputy N.Z. Privacy Commissioner, published two of the earliest formal papers on PIAs, in the Australasian journal Privacy Law & Policy Reporter (Stewart, 1996a,b). Stewart also organised a discussion session on PIAs in Christchurch, New Zealand, on 13 June 1996 including Longworth (1996) (Flaherty, 2000).

In 1996–1997, in the context of public concerns about a driver licensing scheme, the then Commissioner, Bruce Slane, adopted a policy of encouraging PIAs in particular circumstances. In January 1999, the NZPC published a 'Guidance Note in Information Matching Privacy Impact Assessments'. This was restricted in its scope to matching programmes, which are the subject of specific requirements under the Act. The current version of the document is dated 2006. A hard-copy collection of 'Approaches, issues and examples' was published as Stewart (2001), and a further paper appeared as Stewart (2002).

In 2002, the NZPC published a 'Privacy impact assessment handbook' (NZPC, 2002). The handbook acknowledges the authorship of Blair Stewart, prior and parallel work in Alberta, Ontario and British Columbia, and interactions with Hong Kong. It also references prior publications by Stewart (1996a,b, 1999, 2001), Flaherty (2000) and Waters (2001). The New Zealand Commissioner hosted an international symposium on PIAs in 2003.

5.2. *Three provinces of Canada*

As noted in the previous section, the then Privacy Commissioners of Ontario and British Columbia were also very early movers. Alberta moved soon afterwards, and almost all provinces have become active users of PIAs, in name at least.

In *Ontario*, since the late 1990s, the principal driver behind government policy in relation to PIAs was not the privacy oversight body, but a central agency called the Management Board Secretariat (MBS). As early as June 1998, a completed PIA became a pre-requisite for approval of Information and Information Technology (I&IT) project plans submitted for Cabinet approval. Guidelines were published in December 1999 (MBS, 1999). With effect from 2006, the function has been absorbed within the Ministry of Government Services (MGS).

As noted earlier, the academic book Flaherty (1989) included an outline description of what a PIA entailed. During his subsequent term as Privacy Commissioner of *British Columbia* from 1993 to 1999, Flaherty took the opportunity to apply the theory. Within the province's public sector, PIAs of some kind were mainstream, although not mandatory, by the late 1990s. Impetus was provided by a public furore over disclosure of the City of Victoria property value assessments on its public website (Flaherty, 1998).

In 2002, the B.C. Freedom of Information and Protection of Privacy Act was amended such that s. 69(5) requires agencies to conduct PIAs for ''a new enactment, system, project or program''. The process has been supported by guidance since as early as 1998. A database of PIA summaries has been maintained since then, which had reached a count of about 150 by the end of 2007. The scope is limited, however, to the determination of their compliance with the Act, i.e. it is little more than a data protection law compliance check and falls a long way short of being a comprehensive PIA.

In *Alberta*, s. 64 of the Health Information Act, passed in 1999, imposes on public agencies in the health care sector the requirement to conduct PIAs. In devising the process, the architects drew on their background in environmental management. The scope is defined as being ''proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information [that] may affect the privacy of the individual who is the subject of the information''. PIAs are not mandated elsewhere in the Alberta public sector. However a central agency, Services Alberta, provides guidelines in relation to their conduct (SA, 2005).

5.3. *Australia*

In Australia, as indicated above, an early form of PIA referred to as a 'program protocol' was imposed on a particular family of data-matching programs by s. 12 and the associated Schedule to the Data-Matching Program (Assistance and Tax) Act 1990. Non-binding guidelines for application to other data-matching programs were published shortly afterwards (OFPC,

1992). Both sets were prepared by Nigel Waters, Deputy to the then Privacy Commissioner, Kevin O'Connor.

The earliest mention of the term 'PIA' found in Australian sources appears to be a 1995 acknowledgement by the Telecommunications Industry Ombudsman that PIAs had a role to play (referred to in Dixon, 1997). Further stimulation arose from Stewart (1996a,b) which, although authored by a New Zealander, was published in an Australasian journal (Clarke, 1996).

In 1997, a call was made for implementation of PIAs, invoking both Stewart's publications and Flaherty's work in British Columbia (Dixon, 1997). Soon afterwards, descriptions of the PIA process at lesser and greater depth were published in Clarke (1998a,b).

In December 2001, the then Privacy Commissioner, Malcolm Crompton, issued 'Guidelines for agencies using PKI to communicate or transact with individuals' (OFPC, 2001). A draft set of generic guidelines was released for public consultation in 2004, and published in final form by Crompton's successor two years later (OFPC, 2006).

In 2004, the State of Victoria issued a guide (OVPC, 2004). The other major State, New South Wales, is supportive of PIAs but has lacked the resources and government commitment to pursue the matter.

5.4. *Canada*

At federal level in Canada, significant impetus was provided in 2000 by "the highly publicised debacle over Human Resources Development Canada's (HRDC) Longitudinal Labour Force File (LLF) whose … dismantlement, following public complaints about the database, cost the department millions of dollars" (Bloomfield, 2004. See also HRDC, 2000).

Policy responsibility in relation to the conduct of PIAs rests with a central agency, the Treasury Board, which has published guidance and a tool (TBC, 2002a,b, 2003). The guidelines require that "initiatives … comply with privacy requirements and … resolve privacy issues that may be of potential public concern" (TBC, 2002a, p. 4) and the process is accordingly not limited to compliance with privacy laws.

The Office of the Privacy Commissioner has an audit and review function, and an Audit Report containing multiple recommendations for improvements was published in late 2007 (OPCC, 2007).

5.5. *Hong Kong*

In early 2000, the then Privacy Commissioner, Stephen Lau, advised the Immigration Department to conduct a PIA in respect of the planned replacement of the HKSAR ID Card. As a result, the scheme was the subject of a PIA at each of four phases between 2000 and 2004. The first PIA Report was published (Pacific Privacy, 2000), but the subsequent three appear not to have been. Some other PIAs have been undertaken, but no formal guidelines have yet been published.

5.6. *U.S.A.*

It might appear incongruous that the USA has not appeared earlier in this section, given that guidance from the Office of the Privacy Advocate in the Internal Revenue Service (IRS) dates from December 1996. This was reflected over time in similar documents prepared by a range of other agencies, and some further impetus was provided by the Electronic Government Act of 2002. The reason for de-valuing these activities is that their contributions to the development of PIA law, policy and practice have been largely negative.

In the current version of the IRS guidelines, for example, which date from 2000, the language used is expansive, but the actual activity that they require is very limited. The document refers not to the 'conduct' of a PIA but to its 'completion', indicating that it is perceived as a product rather than as a process that influences design. Worse, it is driven from the very limited and patchy provisions in US statutes, and not from an examination of the proposal and its impacts. This is fairly typical of the US federal approach to privacy, which has always been pragmatic and reactive rather than substantive and anticipatory (Bennett, 1992).

The Department of Homeland Security's Privacy Officer has authority under s. 222 of the Homeland Security Act of 2002 to require PIAs. A Privacy Threshold Analysis (PTA) instrument is used to determine whether a PIA is required. The examinations required are so superficial, and so unrelated to actual privacy needs and expectations, that extraordinarily privacy-invasive measures were instituted in a wide range of systems that performed at least nominal roles in the Bush Administration's 'war on terror'. Such activities are PIAs in name only. Their actual form is that of a mere data protection law compliance checklist. With rare exceptions, the USA remains a wasteland from the viewpoint of privacy policy.

Outside government, the ideology of the US private sector is hostile to the notion that consumers might have a participatory role to play in the design of business systems. This is of considerable significance internationally, because US corporations have such substantial impact throughout the world. Their lack of appreciation of the privacy impacts of their operations, and of the annoyance that their arrogance causes, has given rise to substantial clashes between the privacy cultures and legal frameworks of the USA and Europe.

One device for forestalling legislative provisions is the creation and publication of a technical or management standard or code. A US standard for PIAs exists in the form of ANSI (2004); but this was merely a limited response to the provisions of the US Financial Services Modernization Act of 1999 (usually referred to as the Gramm-Leach-Bliley Act). Corporations that wish to sustain the privileged position that they achieved through the FIP movement exist in many countries other than the USA. An international standard is being developed through a committee of the International Standards Organisation: ISO/IEC JTC-1 SC-27 WG-5. As is commonly the case with standards organisations, these processes have lacked the least vestige of consultation with people, or with their representatives or advocates for their interests.

5.7. *States of the U.S.A.*

As late as the end of 2007, there was still very little evidence of PIAs at State level. Even in California (whose population of 36 million is exceeded by only 6 members of the EU, and whose

GDP is much the same as that of the U.K. and of France), the only signs of progress have been a 2006–2007 legislative debate over a Bill that mentioned PIAs, and a bland (and, at the time of writing, unfulfilled) statement by the State's Office of Privacy Protection that it is developing a method and tools for agencies to use.

5.8. *Europe*

The term 'PIA' and the processes that a PIA involves have largely been developed in the Anglophone world. Academic literature searches in 2007 generated virtually no material in the English language focused on PIAs in Member States of the European Union (EU), and a practitioner literature search did no better (ICO, 2007a, Appendix H). The term PIA has certainly been known in some European countries, however, not least The Netherlands. See, for example, Kenny and Borking (2002).

Article 20 of the 1995 EU Directive (EU, 1995), headed 'Prior Checking', states 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''. The requirement appears to have been implemented in the laws of some 17 of the EU nations. The form in which it is expressed is highly varied, however, and the coverage is very patchy. Moreover, the actual extent to which the various laws are respected is far from clear.

In the U.K. in April 2002, a Cabinet Office document advocated the use of PIAs to promote more consistent decision making across public services on privacy and data sharing issues. (Recommendation 19 and Annex D of UKCO, 2002, reported in Stewart, 2002.) In 2007, the U.K. Information Commissioner's Office commissioned a project to deliver a comprehensive review of PIA law, policies and practices around the world (ICO, 2007a, on which this paper has drawn heavily), and a PIA handbook (ICO, 2007b).

At least two other EU countries appear to be moving in the direction of PIAs. Finland has proposed a model that has a resemblance to the PIA models found in Canada, Australia and New Zealand (DPOF, 2007). In addition, the Irish Data Protection Commissioner's Office has recommended the conduct of a PIA in relation to any proposal to apply biometrics in the workplace or school (DPCIE, 2007).

6. Key themes

This section identifies a small set of key themes that arise from a survey of laws, policies and practices relating to PIAs around the world. The themes selected as being of greatest significance are the scope of the PIA concept, the balance between mandation and voluntary conduct of PIAs, and the areas in which PIAs have been applied.

The definitions used in various publications are provided in Appendix 1. In some jurisdictions, especially the USA but also a number of Canadian provinces, the scope is so limited that the activity is not really impact assessment, but merely data protection law compliance audit. In most jurisdictions, however, the scope is reasonably broad, and a PIA is primarily a process, with the PIA Report treated as just one of the deliverables rather than as an end in itself.

In a few cases, the requirement to undertake a PIA has been enshrined in law. Any mandation of PIAs is generally worded carefully, however. Requiring that one be conducted for every project is likely to be counter-productive because it tends to encourage merely formal checklist-filling rather than intellectual engagement with the issues. It is more common for organisations to be required to consider whether a PIA is needed. Hence, in most jurisdictions, PIAs are regarded as an instrument of policy.

In many jurisdictions, the PIA process is motivated by the need for public trust, and is framed in terms of risk management. That was evident in the EU Directive in 1995, and has been commented on by, among others, Raab (2004). The evolution of PIAs needs to be seen within the context of larger trends in advanced industrial societies to manage risk and to impose the burden of proof for the harmlessness of a new technology, process, service or product on its promoters. Personal information systems should be ''regarded as (relatively) dangerous until shown to be (relatively) safe, rather than the other way around'' (Bennett and Raab, 2006, p. 62).

From the late 1990s onwards, PIAs were increasingly recognised as an idea whose time had come. Guidelines have been published, some by privacy oversight bodies, some by central agencies, and others by consultants. Many sets of guidelines are of the nature of checklists, and can easily lead to the generation of documents that evidence a superficial understanding of the privacy issues arising from the project.

Other sets of guidelines, on the other hand, are educational, and intentionally designed to stimulate constructive approaches to what are usually complex and multi-dimensional problems. Placement within the context of risk management is particularly noticeable in the guidelines of Ontario (MBS, 1999), Canada (TBC, 2002b; OPCC, 2007), Alberta (SA, 2005), Australia (OFPC, 2006) and the U.K. (ICO, 2007b). Appendix 3 identifies the sets of PIA guidelines known to the author, classified into recommended authorities, early documents, and other current documents.

The performance of PIAs has to date been predominantly a public sector activity. Many of the guidelines apply equally to the private sector, however, and there are instances in most jurisdictions of the technique being applied at least in the context of public–private partnerships, and in some cases by industry associations and corporations as well.

7. Conclusions

Since its emergence in the mid-1960s, privacy protection has been constrained by the fair information practices model to a framework that has been more protective of corporate and government interests than of people's data, let alone of people themselves. The early emphasis was on bodies of principles that could be applied to individual organisations, business processes, and projects. Among the challenges that confronted this approach were the dominance of the FIP notion, and the enormous diversity of business and government, and of applications of information technologies. The bodies of principles are accordingly riddled with exemptions and

exceptions, and have been continually undermined by subsequent laws.

Since the mid-1990s, PIA has established itself as an important tool. It can be distinguished from processes such as compliance checks and privacy audits because of its anticipatory, positive and risk-management orientations. The PIA meme is already mature in several countries, most notably in Canada and Australia, is making advances in other countries such as New Zealand and the United Kingdom, and has gained a toe-hold in Hong Kong. It may be emergent in countries on the Continent of Europe, although the technique is of course subject to local variants and local naming conventions.

On the other hand, PIAs as defined in this paper are almost non-existent in the USA. In the US public sector, government agencies have subverted the term to refer to a mere legal compliance study; and US private sector philosophies reject the notion that public policy and consumers have a role to play in the design of business systems. The lack of comprehension of privacy issues among US corporations has serious implications, because of their continuing endeavours to apply privacy-invasive technologies and business processes throughout the world, and to negotiate privacy protection laws down to the low level prevalent in their domestic economy.

Outside the USA, PIAs have become an instrument whereby commentators and advocates can demand more information and more consultation, and privacy oversight agencies, despite their dismal lack of formal powers, can argue for deeper consideration of privacy by government agencies and corporations. Organisations perceive PIAs as a means to analyse and manage risk, and it appears that this positive approach may be in the process of overtaking the hostile, reactionary approaches such as industry standards, and attempts to re-kindle the fair information practices movement.

The coming years will tell whether PIAs achieve their aims of surfacing issues, involving the public, and ensuring a multi-stakeholder approach to initiatives. Without PIAs of the kind described in this paper, it will be difficult to achieve appropriate balances among conflicting interests. Return on business technology investments is at risk, because of high levels of distrust by consumers of corporations, and by citizens of governments. PIAs represent an antidote to the problem.

Acknowledgements

A preliminary version of this paper was prepared in February 2004, which formed the basis for a presentation at Queens University, Kingston Ontario, on 9 June 2004. Many people provided assistance during the preparation of that version, including Blair Stewart (NZ), Nigel Waters, Graham Greenleaf, Philip George and Chris Connolly (AU), Ann Cavoukian, David Flaherty, Peter Hope-Tindall, Pierrot Peladeau and Stephanie Perrin (CA), Dave Banisar, Robert Gellman, Lance Hoffman and Willis Ware (US), Herbert Burkert (Germany), and Lee Bygrave (Norway).

The next opportunity to further develop the paper did not arise until the second half of 2007, when a team led by Loughborough University was commissioned by the U.K. Information Commissioner's Office to undertake an international study of laws, policies and practices relating to PIAs around the world (ICO, 2007a), and prepare a PIA handbook (ICO, 2007b). The author greatly appreciates the assistance of his colleagues on that project, Robin Bayley, of Linden Consulting Inc and Prof. Colin Bennett of the University of Victoria, both in Victoria, British Columbia, Andrew Charlesworth of the University of Bristol, and Adam Warren (Project Manager) and Prof. Charles Oppenheim (Project Director), both of Loughborough University. See [2008] 24 CLSR 233–242. The permission of the Information Commissioner's Office's to reproduce relevant material arising from that Study as part of this paper is also acknowledged.

All evaluative comments, however, are the responsibility of the author alone.

Appendix 1. Definitions

Impact assessment is defined by International Association for Impact Assessment (IAIA) as ''the identification of future consequences of a current or proposed action''.

The two earliest definitions of *privacy impact assessment* found in the literature are:

- ''What is a PIA? There is no statutory definition of a PIA in NZ or Australia. Nor is there any internationally accepted definition. To promote discussion I tentatively suggest that a PIA is a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal. An alternative definition might be that a PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated. I should confess that the two definitions are derived from definitions of environmental impact assessment but with the substitution of the word 'privacy' where 'environment' would normally appear. I have chosen to do this not simply for convenience but because I have observed some correlations between environmental impact assessment and privacy impact assessment'' (Stewart, 1996a)
- ''a process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and examined'' (Clarke, 1998b)

The following list of definitions of privacy impact assessment from documents published by national and sub-national privacy oversight agencies draws heavily on ICO (2007a, p. 3):

- New Zealand: PIA is defined as ''a systematic process for evaluating a proposal in terms of its impact upon privacy''
- Canada: PIAs ''provide a framework to ensure that privacy is considered throughout the design or re-design of a programme … [and to] identify the extent to which it complies with all appropriate statutes''. This is done to ''mitigate privacy risks and promote fully informed policy''
- Australia: PIA is an ''assessment of actual or potential effects on privacy, and how they can be mitigated''
- New South Wales: ''PIA involves a comprehensive analysis of the likely impacts of a project upon the privacy rights of

individuals. It is a little … like an environmental impact assessment done for a new development proposal. The assessment can ensure that any problems are identified – and resolved – at the design stage. PIA is not only about ensuring compliance with the relevant information privacy laws (such as the PPIP Act and the HRIP Act), but can also help to minimise the risk of reputational damage by identifying broader privacy concerns (such as bodily or territorial privacy impacts)''
- Alberta: ''A privacy impact assessment (PIA) is a process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy. The process is designed to ensure that the public body evaluates the project or initiative for technical compliance with the FOIP Act and also assesses the broader privacy implications for individuals. A PIA is both a due diligence exercise and a risk-management tool. The PIA process requires a thorough analysis of the potential impact of the initiative on privacy and a consideration of measures to mitigate or eliminate any negative impact. The PIA is an exercise in which the public body identifies and addresses potential privacy risks that may occur in the course of its operations''
- United States of America: ''PIA is an analysis of how information in identifiable form is collected, stored, protected, shared and managed … [to] ensure that system owners and developers have consciously incorporated privacy protection throughout the entire life cycle of a system''

Appendix 2. Exemplars

This Appendix identifies the earliest-known exemplars of PIA Reports, together with sources of PIA Reports in a number of jurisdictions.

Early exemplars

- April 1993, in Australia, re a smart card-based loyalty scheme for Card Technologies Australia Ltd (in this author's consultancy files)
- March 1995, in Ontario, re Intelligent Transportation Systems (IPCO, 1995);
- September 1995 in British Columbia, re Provincial Identity Cards (Flaherty, 1995);
- October 1996 in Australia, re MasterCard Cash (in this author's consultancy files)
- April 1997 in Ontario, re Geographic Information Systems (IPCO, 1997), mirrored in Clarke (1998a,b);
- November 1997 in New Zealand, re photo driver licences (listed in Stewart, 2001)
- March 1998, in N.S.W., re patient data linkage by the Health Commission (in this author's consultancy files)
- June 1998 in New Zealand, re the National Fire and General Insurance Claims Register (listed in Stewart, 2001)
- July 1998 in New Zealand, re the Health Intranet Project (listed in Stewart, 2001)
- February 1999 in New Zealand, re the Mental Health Information Project (Harding, 1999)
- September 2000 in Hong Kong, re the HKSAR ID Card (Pacific Privacy, 2000)

PIA exemplars in Australia – federal

Sections of Appendix E within ICO (2007a,b), and within that:

- Appendix 2: Examples of PIAs by or for Australian Government Agencies (p. 15)
- Appendix 3: Examples of Published PIA Reports by or for Australian Government Agencies (p. 16)
- Appendix 4: Examples of Private Sector PIAs (p. 17)

PIA exemplars in Alberta (but mostly without PIA-relevant content)

The Alberta Privacy Commissioner's PIA Registry is at: http://www.oipc.ab.ca/pia/registry.cfm

PIA exemplars in British Columbia (largely data protection law compliance)

BC's Personal Information Directory containing PIA summaries is at http://www.mser.gov.bc.ca/foipid/public/query.asp?FreeText=on

Data protection law compliance checklist exemplars in the USA

Department of Homeland Security at http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#10
Internal Revenue Service at http://www.irs.gov/privacy/article/0,,id=122989,00.html
US Postal Service at http://www.usps.com/privacyoffice/pialist.htm
Department of Transportation at http://www.dot.gov/pia.html
Department of Labor at http://www.dol.gov/cio/programmes/pia/mainpia.htm
Department of State at http://foia.state.gov/piaOnline.asp
Department of Justice at http://www.usdoj.gov/pclo/pia.htm
Department of Health and Human Services at http://www.hhs.gov/foia/
Department of Education at http://www.ed.gov/notices/pia/index.html
Bureau of the Census at http://www.census.gov/po/pia/

Appendix 3. Guidelines

This Appendix identifies the small set of guidelines recommended by the author, the earliest-known guidelines in relation to the conduct of PIAs, and other known guidelines.

Recommended guidelines

The following small set of guidelines is recommended by the author as a basis for the conduct of PIAs. The set is provided in chronological order, most recent first:

- ICO (2007b), the *U.K. Information Commissioner's Office's* 'Privacy impact assessment handbook'
- OFPC (2006), the Office of the *Australian Federal Privacy Commissioner's* 'Privacy impact assessment guide'
- SA (2005), *Service Alberta's* 'Privacy compliance: privacy impact assessments'
- TBC (2002b), the *Treasury Board Secretariat of Canada's* 'PIA guidelines: a framework to manage privacy risks', subject to implementation of the Privacy Commissioner's Recommendations in OPCC (2007)
- NZPC (2002), the *New Zealand Privacy Commissioner's* 'Privacy impact assessment handbook'
- MBS (1999), the *Ontario Management Board Secretariat's* 'Privacy impact assessment guidelines'

Early guidelines

- SSNYPSC (1991), referred to in Stewart (2001), which states that ''official guidelines for the preparation of PIAs date from at least 1991 … See SSNYPSC (1991)''
- ''sample privacy impact statement'' relating to smart cards (IPCO, 1993)
- 'Suggested rules for evaluating the privacy impacts of emerging technologies', Appendix A to Flaherty (1994) [link active in 2004, but broken in 2007]
- IRS (1996)
- HealthBC (1997)
- joint publications of the Ontario Information Privacy Commissioner and an industry association relating to PIAs for smart card projects (IPCO/ACTA, 1997, 2000)
- Uni Alberta (1998)
- Clarke (1998a,b)

Other current guidelines

The following guidelines, which are adjacent to PIAs, or overly specific, or dated, or are otherwise not recommended by the author, are listed in chronological order:

- US Department of Justice – USDOJ (2000)
- Office of the Information and Privacy Commissioner Alberta – OIPC-AB (2001)
- Office of the Australian Federal Privacy Commissioner – OFPC (2001 – for public key infrastructure projects)
- US Department of the Interior – USDOI (2002)
- US Office of Management and Budget – US OMB (2003)
- Office of the Victorian Privacy Commissioner – OVPC (2004)
- British Columbia Ministry of Labour and Citizens' Services – BC (2006)
- US Department of Homeland Security – US DHS (2007)

Guidance is increasingly appearing in commercial documents and books, such as Karol (2001) and Marcella and Stucki (2003, p. 332–48).

Roger Clarke *(roger.clarke@xamax.com.au) is Principal of Xamax Consultancy Pty Ltd, Canberra and a member of CLSR Editorial Board. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., a Visiting Professor in the E-Commerce Programme at the University of Hong Kong, a Visiting Professor in the Department of Computer Science at the Australian National University and currently Chair of the Australian Privacy Foundation.*

REFERENCES

ANSI. Privacy impact assessment standard. American National Standards Institute; 2004. ANSI X9.99:2004.

APEC. APEC privacy framework. Asia-Pacific Economic Cooperation. Available at: http://www.apec.org/apec/apec_groups/committees/committee_on_trade/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1; 2005.

Becker H, Vanclay F. The international handbook of social impact assessment. Cheltenham: Edward Elgar; 2003.

Bennett CJ. Regulating privacy: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press; 1992.

Bennett CJ, Raab CD. The governance of privacy: policy instruments in global perspective. Cambridge: MIT Press; 2006.

Bloomfield S. The role of the privacy impact assessment. Office of the Privacy Commissioner of Canada. Available at: http://www.privcom.gc.ca/speech/2004/sp-d_040310_e.asp; 2004.

Bygrave L. Data protection law: approaching its rationale, logic and limits. Kluwer Law International; 2002.

BC. Privacy Impact Assessment Process (PIA). Victoria BC: Ministry of Labour and Citizens' Services; 2006. Available at: http://www.cio.gov.bc.ca/services/privacy/Public_Sector/pia/default.asp.

Carter M. Integrated electronic health records and patient privacy: possible benefits but real dangers. Medical Journal of Australia:28–30. Available at: http://www.mja.com.au/public/issues/172_01_030100/carter/carter.html, January 2000;172.

Clarke R. Information technology and dataveillance. Communications of the ACM(5):498–512. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html, May 1988;31.

Clarke R. Computer matching by government agencies: the failure of cost/benefit analysis as a control mechanism. Informatization and the Public Sector. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/MatchCBA.html#CBA 1995a.

Clarke R. A normative regulatory framework for computer matching. Computer & Information Law(4):585–633. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/MatchFrame.html, 1995b;XIII.

Clarke R. Privacy and dataveillance, and organisational strategy. In: Proc. Conf. I.S. Audit & Control Association (EDPAC'96), Perth, 28 May 1996. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/PStrat.html.

Clarke R. Privacy impact assessments. Xamax Consultancy Pty Ltd. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html; 1998a.

Clarke R. Privacy impact assessments. Xamax Consultancy Pty Ltd. Available at: http://www.xamax.com.au/DV/PIA.html; 1998b.

Daniel M, Webber MJ, Wigan MR. Social impacts of new technologies for traffic management. Australian Road Research Board; 1990. Research Report ARR 184.
DPCIE. Biometrics in the workplace. Data Protection Commissioner of Ireland. Available at: http://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm; 2007.
DPOF. Privacy impact assessment. Presentation slides. Data Protection Ombudsman of Finland; August, 2007. Slide 15.
Dixon T. Communications Law Centre wants IPPs revised in line with Australian Privacy Charter. Privacy Law and Policy Reporter 3, 9 (January 1997) 4. Available at: http://www.austlii.edu.au/au/journals/PLPR/1997/4.html.
EU. Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive 95/46/EC. Official Journal:31–50. Available at:, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm, 1995;L 281.
Flaherty D. Protecting privacy in surveillance societies. University of North Carolina Press; 1989.
Flaherty DH. Submission to industry Canada re the information highway. In particular Appendix A. Available at: http://www.oipcbc.org/publications/other/Industry-Canada.html; December 1994 [link active in 2004, but broken in 2007].
Flaherty DH. Provincial identity cards: a privacy-impact assessment. Available at: http://www.oipcbc.org/publications/presentations/identity_cards.html; September 1995 [broken link at 4 February 2004].
Flaherty D. An investigation concerning the disclosure of personal information through public property registries. Office of the Information and Privacy Commissioner of British Columbia. Investigation P98-011. Available at: http://www.oipcbc.org/investigations/reports/invrpt11.html; 31 March 1998.
Flaherty DH. Privacy impact assessments: an essential tool for data protection. In: A presentation to a plenary session on ''New technologies, security and freedom,'' at the 22nd annual meeting of privacy and data protection officials held in Venice, September 27–30, 2000; October 2000. Reprinted in Privacy Law & Policy Reporter November 2000;7(5):85–90. Available at: http://www.austlii.edu.au/au/journals/PLPR/2000/45.html. Revised version in Perrin S, Black H, Flaherty DH, Rankin TM. The personal information protection and electronic documents act. Toronto: Irwin Law; 2001.
Harding E. Privacy impact assessment and commentary on the mental health information project. New Zealand Health Information Service. Formerly at: http://www.nzhis.govt.nz/documentation/mhinc/ak983340.doc; February 1999. Mirrored at: http://www.anu.edu.au/people/Roger.Clarke/DV/NZMentalHlthPIA-9902.html.
HealthBC. Sample privacy impact statement. British Columbia Ministry of Health. Available at: http://www.hlth.gov.bc.ca/him/bc/sc/impact.html; 1997 [broken link at 4 February 2004].
HEW. Records, computers and the rights of citizens. U.S. Dept. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems. Cambridge. Mass.: MIT Press. Available at:, http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm; 1973.
Hoffman L. Security and privacy in computer systems. Los Angeles, California: Melville Publishing Co. (A Division of Wiley); 1973.
HRDC. HRDC dismantles longitudinal labour force file databank. Human Resources and Social Development Canada. Available at: http://www.hrsdc.gc.ca/en/cs/comm/news/2000/000529_e.shtml; 29 May 2000.
IAIA. Principles of environmental impact assessment best practice practice. International Association for Impact Assessment, in Cooperation with U.K. Institute of Environmental Assessment. Available at: http://www.iaia.org/Members/Publications/Guidelines_Principles/Principles%20of%20IA.PDF; January 1999.
IAIA. Social impact assessment: international principles. International Association for Impact Assessment. Available at: http://www.iaia.org/Members/Publications/Guidelines_Principles/SP2.pdf; May 2003.
ICO. Privacy impact assessments: international study of their application and effects. Wilmslow, U.K.: Information Commissioner's Office. Available at: http://www.ico.gov.uk/Home/about_us/research/data_protection.aspx; 2007a.
ICO. Privacy impact assessment handbook. Wilmslow, U.K.: Information Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html; 2007b.
IOCSIA. Guidelines and principles for social impact assessment (U.S. Department of Commerce, National Oceanic and Atmospheric Administration, and National Marine Fisheries Service). Interorganizational Committee on Guidelines and Principles for Social Impact Assessment. Available at: http://www.iaia.org/Members/Publications/Guidelines_Principles/SIA%20Guide.PDF; May 1994.
IPCO. Smart cards. Information and Privacy Commissioner/Ontario. Available at: http://www.ipc.on.ca/index.asp?navid=46&fid1=331&fid2=4; April 1993.
IPCO. Suggested changes to the municipal freedom of information and protection of privacy act: submission to the standing committee on the legislative assembly. Information and Privacy Commissioner/Ontario. Available at: http://www.ipc.on.ca/index.asp?layid=86&fid1=227; January 1994.
IPCO. Eyes on the road: intelligent transportation systems and your privacy. Information and Privacy Commissioner/Ontario. Available at: http://www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/its-e.htm; March 1995 [broken link at 4 February 2004].
IPCO. Appendix to 'Geographic information systems'. Information and Privacy Commissioner/Ontario. Available at: http://www.ipc.on.ca/images/Resources/gis.pdf; April 1997. and mirrored in Clarke (1998a,b).
IPCO/ACTA. Smart, optical and other advanced cards: how to do a privacy assessment. Information and Privacy Commissioner/Ontario and Advanced Card Technology Association of Canada. Available at: http://www.ipc.on.ca/images/Resources/up-cards.pdf; September 1997.
IPCO/ACTA. Multi-application smart cards: how to do a privacy assessment. Information and Privacy Commissioner/Ontario and Advanced Card Technology Association of Canada. Available at: http://www.ipc.on.ca/index.asp?navid=46&fid1=414&fid2=4; August 2000.
IRS. IRS privacy impact assessment. Office of the Privacy Advocate, Internal Revenue Service. Version 1.3, as adopted by the [U.S.] CIO Council in February 2000. Available at: http://www.cio.gov/Documents/pia_for_it_irs_model.pdf; December 1996.
ISO/IEC JTC-1 SC-27 WG-5. Identity management and privacy technologies committee. Listed at: http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306.
Karol TJ. Cross-border privacy impact assessments: an introduction. Information Systems Control Journal. Available at: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17226&TEMPLATE=/ContentManagement/ContentDisplay.cfm, March 2001;3.
Kenny S, Borking J. The value of privacy engineering. Refereed article. The Journal of Information, Law and Technology (JILT)(1). Available at:, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/, 2002;2002.

Longworth L. Telecommunications and privacy issues; 1992. Report for the N.Z. Ministry of Commerce.
Longworth E. Notes on privacy impact assessments. Christchurch, NZ: Privacy Issues Forum; 13 June 1996. in NZPC (1997).
Marcella AJ, Stucki C. Privacy handbook: guidelines, exposures, policy implementation, and international issues. Wiley; 2003.
MBS. Privacy impact assessment guidelines. Revised 2001. Management Board Secretariat, Government of Ontario. Available at:, http://www.accessandprivacy.gov.on.ca/english/pia/index.html; 1999.
NSWPC. Guidelines for the operation of personal data systems. Sydney: N.S.W. Privacy Committee. Document BP31. Available at: http://www.anu.edu.au/people/Roger.Clarke/DV/NSWPCGs.html; April 1977.
NZPC. A compilation of materials in relation to privacy impact assessment. New Zealand Privacy Commissioner; 1997.
NZPC. Privacy impact assessment handbook. Office of the New Zealand Privacy Commissioner. Available at: http://www.privacy.org.nz/privacy-impact-assessment-handbook/; March 2002.
OECD. Guidelines on the protection of privacy and transborder flows of personal data. Paris: Organisation for Economic Cooperation and Development. Available at: http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html; 1980.
OFPC. The use of data matching in commonwealth administration – guidelines. Office of the Federal Privacy Commissioner. Rev. February 1998. Available at: http://www.privacy.gov.au/publications/dmcomadmin.pdf; 1992.
OFPC. Privacy and public key infrastructure: guidelines for agencies using PKI to communicate or transact with individuals. Office of the Federal Privacy Commissioner. Available at: http://www.privacy.gov.au/publications/pki.doc; December 2001.
OFPC. Privacy impact assessment guide. Office of the Federal Privacy Commissioner. Available at: http://www.privacy.gov.au/publications/PIA06.pdf; August 2006.
OIPC-AB. Privacy impact assessment: instructions and annotated questionnaire. Canada: Office of the Information and Privacy Commissioner Alberta. Available at: http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf; January 2001.
OPCC. Assessing the privacy impacts of programs, plans, and policies. Office of the Privacy Commissioner of Canada. Available at: http://www.privcom.gc.ca/information/pub/ar-vr/pia_200710_e.pdf; October 2007.
OTA. Technology assessment in business and government. Office of Technology Assessment. NTIS order #PB-273164. Available at: http://www.princeton.edu/~ota/disk3/1977/7711/7711.PDF; January 1977.
OVPC. Privacy impact assessments – a guide. Office of the Victorian Privacy Commissioner. Available at: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf; August 2004.
Pacific Privacy. Hong Kong special administrative region identity card project – report on initial privacy impact assessment. Pacific Privacy Pty Ltd. Available at: http://www.legco.gov.hk/yr00-01/english/fc/esc/papers/esc27e1.pdf; November 2000.
Porter AL, Rossini FA, Carpenter SR. A guidebook for technology assessment and impact analysis. Elsevier; 1980.
PPSC. Personal privacy in an information society. Privacy Protection Study Commission. Washington, D.C.: U.S. Government Printing Office. Available at:, http://epic.org/privacy/ppsc1977report/; July 1977. , http://aspe.hhs.gov/datacncl/1977privacy/toc.htm.
Raab C. The future of privacy protection. London: Office of Science and Technology. Available at: http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/The_Future_of_Privacy_Protection/The_Future_of_Privacy_Protection.html; 2004.
Rule JB. Private lives and public surveillance: social control in the computer age. Schocken Books; 1974.
Rule JB, McAdam D, Stearns L, Uglow D. The politics of privacy. New American Library; 1980.
SA. Privacy compliance: privacy impact assessments. Service Alberta. Available at: http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3; 2005.
SSNYPSC. Statement of policy on privacy in telecommunications. State of New York Public Service Commission; 22 March 1991. Reprinted in Information and Privacy Commissioner of Ontario submission to the Ontario Telephone Service Commission 'Privacy and Telecommunications', September 1992.
Stewart B. Privacy impact assessments. Privacy Law & Policy Reporter(4):61–4. Available at: http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/39.html, 1996a;3.
Stewart B. PIAs – an early warning system. Privacy Law & Policy Reporter(7):134–8. Available at: http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/65.html, 1996b;3.
Stewart B. Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies. Privacy Law & Policy Reporter(8):147–9. Available at: http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1999/8.html, February 1999;5.
Stewart B. Privacy impact assessment: some approaches, issues and examples. Proc. Conf. Privacy. N.Z. Privacy Commissioner; 2001.
Stewart B. Privacy impact assessment roundup. Privacy Law & Policy Reporter(5):90–1. Available at: http://www.austlii.edu.au/au/journals/PLPR/2002/41.html, October 2002;9.
TBC. Privacy impact assessment policy. Treasury Board of Canada Secretariat. Available at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp; 2002a.
TBC. Privacy impact assessment guidelines: a framework to manage privacy risks. Treasury Board of Canada Secretariat. Available at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp; 2002b.
TBC. Privacy impact assessment (PIA) e-learning tool. Ottawa: Treasury Board Secretariat. Available at: http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp; October 2003.
UKCO. Privacy and data-sharing: the way forward for public services: Annex D: the analytical framework and privacy impact assessments. UK Cabinet Office Strategy Unit. Available at: http://www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/strategy/piu-data.pdf; April 2002 [Annex D was at: http://www.piu.gov.uk/2002/privacy/report/annex-d.htm, link active in 2004, but broken in 2008].
UNEP. Environmental impact assessment training resource manual. 2nd ed. United Nations Economics and Trade Programme. Available at: http://www.unep.ch/etu/publications/EIAMan_2edition_toc.htm; June 2002.
Uni Alberta. Privacy impact assessment model. University of Alberta. Available at: http://www.ualberta.ca/FOIPP/mud/s212a.htm; 1 April 1998 [link active in 2007, but broken in 2008].
USDOC. Safe harbor. U.S. Department of Commerce. Available at: http://www.export.gov/safeharbor/sh_documents.html; 2000.
USDOI. Privacy impact assessment and guide. Department of the Interior. Available at: http://www.doi.gov/ocio/privacy/Privacy_Impact_Assessment_9_16_02.doc; July 2002.
USDOJ. Privacy impact assessment for justice information systems. Working paper. Available at: http://www.ojp.usdoj.gov/archive/topics/integratedjustice/piajis.htm; August 2000 [link active in 2004, but broken in 2008].
US OMB. E-Government Act Section 208 Implementation Guidance. Washington DC: Office of Management and Budget; September 26, 2003. Available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

US DHS. Privacy Impact Assessments - Official Guidance. Washington DC: Department of Homeland Security; May 2007. Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.
Warren A, Bayley R, Bennett C, Charlesworth A, Clarke R, Oppenheim C. Privacy impact assessments: international experience as a basis for UK guidance. Computer Law & Security Report April–June 2008;24(3):233–42.
Waters N. Privacy impact assessment – traps for the unwary. Privacy Law & Policy Reporter(9):176. Available at: http://www.austlii.edu.au/au/journals/PLPR/2001/10.html, February 2001;7.
Westin AF. Privacy and freedom. Atheneum; 1967.
Westin AF, editor. Information technology in a democracy. Cambridge, Mass: Harvard University Press; 1971.
Westin AF, Baker MA. Databanks in a free society: computers, record-keeping and privacy. Quadrangle; 1974.

All items for which URLs are provided were most recently accessed on 2 February 2008, unless otherwise noted.