# Privacy Impact Assessment in Australian Contexts

Roger Clarke

---


## Abstract

Privacy impact assessment (PIA) is a systematic process for evaluating the effects on privacy of a proposed system or scheme or draft legislation. It is proactive and open-ended in nature, rather than a mere check of compliance with existing laws or post-implementation audit. PIAs have become mainstream in Australia, despite the hostile politico-legal contexts in which they are applied.

This paper provides outlines of the privacy laws that apply to the public sectors of the Commonwealth, the six States and two Territories, plus the rather complex situation applying to the private sector. It then examines the development of PIA processes within those ten contexts. PIAs are shown to be a vital mechanism that is capable of both serving organisations' needs for risk assessment and partially compensating for the serious shortfall in the privacy protections available to Australian consumers and citizens.


---

## 1. Introduction

Privacy has been a major concern for several decades. Privacy harm may be subtle, and the ways in which the harm arises may be non-obvious. It is therefore important that studies be undertaken to identify the factors that give rise to privacy invasions. Once systems are in place, it is expensive and difficult to adapt them. Those studies should therefore be undertaken prior to the design and implementation of systems, or at the very least in parallel with and as part of their design and implementation. The term commonly used to refer to such studies is 'privacy impact assessment' (PIA). This paper surveys PIA in the variety of jurisdictional contexts that exist in the Australian federation.

Privacy has been an ongoing issue in Australia at least since Zelman Cowen delivered his ABC Boyer Lecture Series (Cowen 1969). The then N.S.W. Attorney-General John Madison commissioned a report from Law Professor Bill Morison. Based on the approach proposed in Morison (1973), Clarke (2006a) discusses privacy's significance together with the following working definition:

> ***Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations***

The term 'privacy' is used in a great many senses, and it is therefore important to underline its multi-dimensionality Clarke (2006a):

- Privacy of the Person, sometimes referred to as 'bodily privacy', is concerned with the integrity of the individual's body, and encompasses the repugnance and ineffectiveness of torture, the right to medical treatment, and issues such as compulsory immunisation, imposed treatments, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement;
- Privacy of Personal Behaviour, including what is sometimes referred to as 'media privacy' encompasses not only sexual preferences and habits, political activities and religious practices but also the reasonable expectation of privacy rights even in 'public places';
- Privacy of Personal Communications, including what is sometimes referred to as 'interception privacy', relating to the use of various channels and media without routine monitoring by others, and including such issues as mail 'covers', use of directional microphones and 'bugs' with or without recording apparatus, telephonic interception and recording, and third-party access to email-messages;
- Privacy of Personal Data, sometimes referred to as 'data privacy' and 'information privacy' – the most common narrow usage of the term.

Morison concluded that such privacy protections as existed were incidental rather than intentional, and that further study and experience were needed before any substantive legal protections were enacted. To enabled this to be achieved, he recommended the establishment of a permanent Committee and staff, with responsibilities to undertake research and handle complaints. The Morison report resulted in the N.S.W. Privacy

Committee Act 1975, which created a complaints-investigation and research organisation. Although Morison's report was presented to the Standing Committee of Attorneys-General (SCAG), no other jurisdiction directly acted on its recommendations.

However, in 1976, the Fraser Government provided a reference to the Australian Law Reform Commission (ALRC). Uncharacteristically, it fumbled the ball very badly. It took seven years to produce its Report (ALRC 1983). By that time Fraser was gone, and it was presented to the subsequent Hawke Government, which, it transpired, was strongly anti-privacy in its orientation (Greenleaf & Nolan 1986, Clarke 1987).

Other countries had moved far less slowly, with the German Land of Hesse in 1970 and Sweden in 1973 leading the world in creating privacy protection laws. Business and government around the world feared that privacy laws might stultify domestic economic activities and that differential privacy laws might harm the burgeoning international trade in personal data. The OECD established its 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', whose primary purpose was 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, p.7). Australia acceded to the OECD Guidelines in 1984.

Consistently with sponsors' aims, the OECD Guidelines provided only limited protection for privacy. Rather, they became the cornerstone of the 'fair information practices' (FIP) movement. The origins of FIP lie in the foundation work of Westin (Westin 1967, 1971; Westin & Baker 1974). The Westin thesis was that the invisible economic hand of business and government activity would ensure that IT did not result in excessive privacy invasion. Hence privacy regulation was unnecessary. To the extent that regulation was imposed, it was vital to minimise the detrimental effects on business and government. FIP-based privacy regimes have been described as an 'official response' which legitimated dataveillance measures in return for some limited procedural protections (Rule 1974, Rule et al. 1980).

Over the 40 years since Westin's foundation work, organisations have perceived their interests to dictate the collection, maintenance and dissemination of ever more data, ever more 'finely grained'. This 'information-intensity' phenomenon has arisen from the increasing scale of human organisations, making them more remote from their clients, and more dependent on abstract, stored data rather than personal knowledge. Other factors have been an increasing level of education among organisations' employees, the concomitant trend toward 'scientific management' and 'rational decision-models' based on detailed criteria and a significant amount of data, and the brisk development in information technology (Clarke 1988).

The FIP approach, as codified in the OECD Guidelines, has provided the basis for virtually all privacy legislation since then. So dominant have corporate and government interests been that several attempts have been made to reduce even the already seriously inadequate provisions that the OECD Guidelines embody. Notable among them have been the U.S. Administration's 'safe harbor' provisions (USDOC 2000) and the APEC Privacy Framework (APEC 2005). During 2007, US corporations led by Microsoft and Google sought to use the low-grade APEC provisions to 'ratchet down' the protections in key countries that have OECD-style protections.

As the preceding discussion shows, the legal framework within which the Privacy Impact Assessment process has developed has not been motivated by the protection of privacy, but rather by the protection of the apparent interests of business and government. The position that corporations and government agencies have long adopted is that PIAs are undesirable, because they may result in the exposure of privacy-negative impacts and hence pressure may accumulate forcing organisations and legislatures to do something about those impacts.

Despite this, the method for conducting PIAs has matured, and is increasingly being applied. How could a technique that is in the politically weak 'public interest' swim against the tide of business and government dominance?

The answer lies in increasing public awareness of the explosion in privacy-invasive information technologies, and the increasing public appreciation that corporations and government agencies are gathering enormous power over consumers and citizens, and are wielding it. Many schemes depend for their effectiveness on their adoption by the scheme's victims. Those victims have been less compliant than organisations would have liked; and occasional media break-outs have given a variety of schemes and technologies a seriously bad name. Faced, with project failures and with an inability to achieve return on substantial investments in technology and systems, organisations have been re-considering what their own interests really are. PIAs are being harnessed as risk management tools, to identify privacy-invasive aspects of projects that can be avoided or mitigated.

PIA methods have reached a sufficient degree of maturity and stability that a survey article is appropriate. The opportunity for this paper was provided by a consultancy assignment commissioned by the U.K. Information Commissioner's Office. A Study of PIA laws, policies and practices around the world was undertaken by a team led by Loughborough University, resulting in ICO (2007a), summarised in Warren et al. (2008). The second deliverable from the assignment was the PIA Handbook (ICO 2007c). The team has since prepared a journal article on the history of PIAs (Clarke et al. 2008).

The examination of PIAs in Australian jurisdictions (ICO 2007b) provided an important source of material reported below. This paper commences with a brief review of the ten jurisdictional contexts within which PIAs are conducted in Australia. It then provides a brief overview of the purpose, process and outcomes of PIAs. Experience in Australia is described, and local sources of guidance are discussed.

---

## 2. Privacy Protection in Australia

The practice of PIAs is highly dependent upon the legal context within which they are undertaken. Ten such contexts can be readily identified in Australia. Each of the nine Crowns is responsible for regulation of its own public sector. The private sector is subject to aspects of Commonwealth law distinct from that which applies to the Commonwealth public sector, and some activities are also subject to, in part conflicting, laws of the States and Territories.

This section provides an outline of privacy protection laws. It is written by a non-lawyer, and is necessarily superficial. Its purpose is to provide a framework within

which practices relating to PIAs can be described. The material has been consolidated from a variety of resources, including the author's prior papers, APF (2007), Caslon (2007), OVPC (2007) and OFPC (2007). Secondary references include Hughes (1991), Tucker (1992), Gunning (2001) and PLPR (1994-2006). Works that express a sceptical view about the worth or appropriateness of privacy protection laws include Doyle & Bagaric (2005) and Mason (2006).

## 2.1 Human Rights Law

Privacy is acknowledged as a human right, under Article 12 of the Universal Declaration of Human Rights (UDHR 1948), and Article 17 of the International Covenant on Civil and Political Rights (ICCPR 1976), both of which use the same form of words:

> ***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.***

Australia has failed to provide constitutional protection for privacy, and, despite the efflux of decades, only one Territory and one State have implemented any statutory protections for human rights. The A.C.T. Human Rights Act (2004), at s.12, provides people with "the right to not to have their privacy, family, home or correspondence interfered with unlawfully or arbitrarily" and "the right not to have his or her reputation unlawfully attacked". The Victorian Charter of Human Rights and Responsibilities Act (2006), in s.13 contains a virtually identical provision.

To date, neither appears to have resulted in any actual change in the behaviour of organisations in relation to privacy. Indeed they appear to have been expressly designed to avoid 'public interest' interference with the right of majority governments to legislate. They provide image without substance, because they create no effective legal mechanism whereby unjustified breaches of human rights can be pursued.

## 2.2 Generic Privacy Protection Laws

No Australian jurisdiction has implemented generic privacy protection laws. The closest to it was the N.S.W. Privacy Committee Act 1975. This created a complaints-investigation and research organisation of broad scope. That statute was rescinded in 1998-99 by the Privacy And Personal Information Protection Act, which replaced the Committee with the far narrower and only marginally more powerful N.S.W. Privacy Commission.

A considerable array of laws provide incidental protections for various aspects of privacy. For example, privacy of the physical person enjoys protection from aspects of the criminal law (e.g. assault, kidnapping and false imprisonment). Privacy of personal behaviour is subject to laws relating to listening devices, cameras and surveillance devices generally. The privacy of personal communications is protected by laws relating to the mail, the recording of conversations, and telephonic and other forms of electronic interception. The privacy of personal data benefits from aspects of the laws of confidence and negligence, and anti-discrimination legislation.

Government agencies are subject to particular provisions in the statutes that govern their activities and programmes. Organisations in both the public and private sectors are subject to provisions within statutes that regulate such activities as public health, education, family law, children's safety, occupational health and safety, financial services, consumer rights, and archives. Many of these laws contain features that are intentionally or at least incidentally privacy-protective, although very few are even faintly comprehensive, and the pattern as a whole is anything but coherent. Delegated legislation such as formal Codes play a role, and some limited benefits arise from informal industry codes and from industry standards.

## 2.3 Data Protection Laws

Several jurisdictions have passed laws that relate specifically to the privacy of personal data. Some use the descriptive titles 'data protection', 'data privacy' or 'information privacy', whereas others misleadingly use the generic term 'privacy'. This sub-section outlines the legislation and identifies relevant privacy oversight agencies. The descriptions are divided into three sub-sections, reflecting the alternative approaches that have been adopted.

### (1) A Data Protection Act and Commissioner

An approach adopted in many countries around the world is to legislate a set of 'data protection principles', and create a data protection oversight body, usually with very limited powers. The framework for most legislative principles is provided by the OECD Guidelines (1980).

The Commonwealth public sector is subject to the Privacy Act 1988, which embodies in s. 14 the Information Privacy Principles (IPPs), and which created the Privacy Commissioner and the Office of the Privacy Commissioner (referred to ambiguously as OPC, and more conveniently as OFPC).

The original draft of the Act (Privacy Bill 1986) was thrown together by public servants at short notice, in an attempt to provide a veneer of respectability for the Australia Card Bill (Greenleaf & Nolan 1986, Clarke 1987). It was the subject of considerable parliamentary negotiation. From the viewpoint of privacy protection, it was a weak instrument, but somewhat better than nothing at all. With the passage of time and of a vast fleet of subsequent laws that over-ride the protections it provided, it has atrophied into an extremely weak instrument.

The private sector nationwide is subject to amendments to the Privacy Act which were embodied in the Privacy Amendment (Private Sector) Act 2000. This created in Schedule 3 the National Privacy Principles (NPP), which are significantly different from the IPPs that apply to the Commonwealth public sector. The Privacy Commissioner's limited oversight powers apply to this segment of the Act as well.

During 1999, the then Attorney-General (Darrell Williams) had called into life a 'Core Consultative Group' (CCG) comprising representatives of industry associations and public interest advocacy groups. It was asked to negotiate a draft Bill and did so, presenting it to the Attorney-General late that year. The Bill that Williams took to the Parliament bore no relationship whatsoever with that which had been negotiated. In parallel with the CCG, a different Bill was prepared by staff of the Department in

collaboration with two industry associations, to the exclusion of privacy advocates. Given this gross breach of trust, it is unsurprising that the provisions served the perceived self-interests of the industry sectors that drafted it, legitimised privacy-invasive practices, and have reduced the levels of privacy protection rather than increasing them (Clarke 2001).

The credit reporting sector nationwide has long been subject to specific provisions enacted in 1989 and contained in ss. 18A-18B and Part IIIA (ss. 18C-18V) of the Privacy Act. For the last 20 years, these have been the subject of continual lobbying by the monopoly credit reference company and the financial services sector, to date with very limited success.

Around 2000, considerable unrest among consumers resulted in effective consultative processes that led to the regulation firstly of unsolicited email by the Spam Act 2003, and secondly of unsolicited tele-marketing calls by the Do Not Call Register Act 2006. The Spam Act is widely regarded as being appropriately-balanced, but will remain largely ineffective unless and until it becomes the basis for a multilateral convention. The Do Not Call Register attracted more than 200,000 registrations in the first 24 hours it was open, and passed 2 million registrations within the first six months, even though it fails to control charities, researchers and politicians.

A review of the Privacy Act, conducted by the ALRC in 2006-08, (ALRC 2007) has proposed some rationalisation of the Privacy Act's provisions, including the consolidation of the rather different sets of Principles into a single set of Unified Privacy Principles (UPPs). The aspects directly relating to PIAs are discussed later in the paper.

Meanwhile, in N.S.W., the Privacy and Personal Information Protection Act (PPIPA) was prepared in 1998 by the bureacracy for the bureaucracy and passed by the Parliament. It embodies a set of Information Protection Principles in ss. 8-19. It replaced the longstanding Privacy Committee with a Privacy Commissioner and Office conveniently referred to as Privacy NSW or NSWPC. The law is perhaps the least privacy-protective of such statutes anywhere in the world, and the Commissioner perhaps the weakest. The Commission has been ignored by successive Governments and starved of resources, and has had very limited impact on privacy-invasive practices in the N.S.W. public or private sectors.

A N.S.W. Health Records and Information Privacy Act was passed in 2002. It affects both public and private sector organisations active in the N.S.W. health care sector. Despite its permissive nature, it was inconvenient to the conduct of a major trial of electronic health records in the Hunter Valley called HealtheLink so the government simply suspended the inconvenient principle. Privacy protections in N.S.W. are nominal rather than real.

The position in Victoria is somewhat different. The Information Privacy Act was drafted by a Data Protection Advisory Council formed by the Minister for Multimedia in 1996. (The author of this paper was a member of that Council). Despite a change of Government in the meantime, the Bill was passed virtually unchanged in 2000. It is a straightforward implementation of the OECD Guidelines, and the approach is therefore dated but mainstream. It established a set of Information Privacy Principles, and a Privacy Commissioner and Office, referred to as Privacy Victoria or OVPC.

The Victorian Health Records Act was passed in 2001. This includes a set of Health Privacy Principles which is highly permissive of data disclosures. The law is administered by the Health Services Commissioner. It encompasses both public and private sector organisations active in the Victorian health care sector.

The A.C.T., after self-government was forced on it by the Commonwealth Parliament in 1988, adopted the Commonwealth Privacy Act. This was done by means of the Australian Capital Territory Government Service (Consequential Provisions) Act 1994 (Cth), in particular s. 23, Schedule 2 and Schedule 3. As a result, the Office of the Federal Privacy Commissioner is supposed to perform the functions of an A.C.T. Privacy Commissioner. There is, however, only limited evidence of much being done, almost all of it within the Commissioner's Annual Reports.

(2) An Information Act and Commissioner

It is common for government agencies to administer their obligations under Freedom of Information and Data Protection laws from within the same organisational sub-unit. This approach is reflected in the constitutions of the oversight agencies in several large jurisdictions, including the U.K. and Ontario.

The Northern Territory adopted this approach for the pragmatic reason of cost-minimisation in administering a tiny population scattered across a vast area. The architect of the Information Act 2002 had been deeply involved in the preparation of the Victorian Information Privacy Act, and the N.T. statute is accordingly a clean and practical application of the (now badly dated) OECD 1980 provisions. The Act created the statutory post of Information Commissioner.

In Western Australia, an Information Privacy Bill was introduced into the Parliament by the Attorney-General in March 2007. It would expand the functions of the existing, small Information Commissioner's Office (which is responsible for the administration of FOI laws) to that of a Privacy and Information Commissioner. Further, it would enable the position to be held concurrently with that of Parliamentary Commissioner (Ombudsman). It is not clear whether any additional resources would be provided to enable the new functions to be addressed. During 2007, the Government was embroiled in political difficulties arising from accusations of engrained corruption, and hence, at the time of writing, the Bill had not progressed.

(3) Bureaucratic Approaches

It is unusual in economically advanced jurisdictions for Parliaments to have taken no legislative action in relation to privacy protection. Four Australian States are among the few laggards.

In Queensland, an unenforceable code exists, in the form of a State Government Standard No. 42 (Sep 2001) and a special one – Standard No. 42A – for the Qld Dept of Health. It is administered by a small Privacy Unit within the Department of Justice and Attorney-General. The Department uses the label 'Queensland Privacy' for the web-page, but whereas in NSW and Victoria that form of title indicates a government agency with at least some degree of independence, in this case it appears to be a slogan or brandname. The arrangements are supposed to be reviewed periodically, but this does

not appear to actually happen. A Parliamentary Report was tabled in April 1998. Like the Standards and the supervisory unit, the Report appears to have had very little effect.

In South Australia, a Cabinet Administrative Instruction (SADPC 1989) establishes a set of Information Privacy Principles and requires agencies to comply. Although nominally binding, it is unclear by what means and by whom it could be enforced. A Privacy Committee of S.A. exists, but its primary function appears to be to approve exemptions to the non-statutory principles. It is unclear whether the Instruction applies to local government. Much the same issues arise with respect to a Department of Health Code of Fair Information Practice (SADOH 2004), which embodies unspecified reductions in the protections declared in the Cabinet Instruction. A Department of Families and Communities Code appears to be identical to that of the Department of Health.

In Tasmania, the Personal Information Protection Act was passed in 2004. Schedule 1 includes a set of Personal Information Protection Principles. There is no privacy oversight agency, however. The Ombudsman can investigate complaints, but cannot enforce his findings. Several years after the Act was passed, neither the Ombudsman nor the Tasmanian public have displayed any interest in such purely nominal powers.

In Western Australia, it appears that, to date, no agency has ever had any substantive function that approximates to a privacy oversight role. The Office of eGovernment has, however, recognised the risks that privacy-invasiveness entails for the adoption of electronic forms of government service delivery.

Legally enforced data privacy safeguards in these four jurisdictions, with a total population of about 8 of Australia's c. 20 million population, are close to non-existent.

---

## 3. The Nature of the PIA Process

The preceding section described the jurisdictional contexts within which PIAs have developed in Australia. This section completes the groundwork needed to support a description of that development by defining the notion of a PIA and distinguishing it from such other processes as a privacy strategy, a privacy issues analysis, a privacy audit, an internal cost/benefit analysis or internal risk assessment, a privacy impact statement, and a legal compliance study.

The most commonly-cited definition of a PIA is "a systematic process for evaluating a proposal in terms of its impact upon privacy" (NZPC 2002). Deputy NZ Commissioner Blair Stewart, who is primarily responsible for that formulation, makes clear that the expression is strongly derivative from the long-established environmental impact assessment arena (Stewart 1996a).

Clarke et al. (2008) distinguishes PIAs from other processes, and identifies the key characteristics of a PIA, as follows:

- 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 focussed 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 present a chronological description of the development of PIAs in Australia, followed by an outline of the guidance that is available to enable their effective planning and conduct.

---

## 4. PIAs in Australia

The development path within Australia can be usefully separated into the periods before and after 2000.

### 4.1 Pre-2000

The earliest activity in Australia that has been identified as being of the nature of a PIA was the 'program protocol' required from 1990 onwards by the Data-Matching Program (Assistance and Tax) Act and expressed in Schedule 1. These requirements were specific to the so-called 'Parallel Data-Matching Program' (Clarke 1994). Generic guidelines for data matching programs, which also had a program protocol at the core, were published in 1992 (current version of February 1998, i.e. unrevised in a decade). But the generic guidelines were not, and still are not, in any way binding on the agencies that conduct them. These were released during Kevin O'Connor's long period as Privacy Commissioner, but the primary responsibility for their development lay with his Deputy, Nigel Waters.

The next activity that has been located is an April 1993 strategy devised by this author as part of a consultancy assignment for a smartcard-based loyalty scheme for Card Technologies Australia Ltd (subsequently re-structured as the NASDAQ-listed Catuity Inc.). 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).

Articles published by the Deputy New Zealand Privacy Commissioner in the Australian Privacy Law & Policy Reporter provided a stimulus to developments (Stewart 1996a, 1996b). In mid-1996, Stewart organised an discussion session on PIAs in Christchurch (Flaherty 2000). See also NZPC (1997) and Stewart (1999).

Also in 1996, this author conducted assignments for the Australian Commission for the Future in relation to smartcard-based payment schemes generally, and for MasterCard International's smartcard-based electronic cash trial (whose international pilot was run in Canberra). Soon afterwards, a call was made by a research group, the Communications Law Centre, for PIAs to be conducted in relation to "any new system, technology or practice which may affect personal privacy" (Dixon 1997). The call invoked Stewart's publications, Flaherty's work in British Columbia, and the Australian Privacy Charter (APC 1994).

During 1998, this author undertook further assignments relating to patient data linkage by the N.S.W. Health Commission, to the then-emergent Australian Business Number and Register, and to a proposed multi-purpose smart identification card for Centrelink. On the basis of the experience accumulated to that point in time, descriptions of the PIA process were published at lesser and greater depth, in Clarke (1998a, 1998b).

### 4.2 Post-2000

The tempo picked up from this time onwards. As indicated in Waters (2001), "there [was] nothing particularly new or radical about PIAs — just a new name for a technique of assessment which privacy regulators and consultants have been performing for years. It is essentially just a systematic appraisal of the privacy implications of a new proposal. Some appraisals are limited to assessing compliance with specific privacy rules or standards, but others range more widely over all privacy issues of concern to affected individuals, whether or not they are currently subject to privacy law". A hard-copy collection of 'Approaches, Issues And Examples' was published as Stewart (2001), and a further paper appeared as Stewart (2002).

In December 2001, the then federal Privacy Commissioner, Malcolm Crompton, issued guidelines relating to a specific category of projects, which included a recommendation that a PIA be performed (OFPC 2001). Although non-binding, those guidelines have been heeded in a number of subsequent projects performed by government agencies. By 2003, the Commissioner had submitted to a Parliamentary Committee that "Commonwealth agencies [should] be required to undertake privacy impact assessments at the beginning of the development of new proposals and initiatives involving the handling of the personal information of the Australian community. These assessments should be published ..." (OFPC 2003, pp. 19-20).

As further discussed below, the Commissioner's Office developed draft PIA Guidelines during 2003-04, and, following a consultation period, published them (OFPC 2006).

During their launch in August 2006, the then Attoney-General (Phillip Ruddock) said that "as a matter of good business practice, I strongly encourage government agencies to use the guide to assist them in playing a larger role in promoting privacy compliance" (AG 2006). This was reinforced in April 2007, when the head of the Attorney-General's Department wrote to all agency heads in relation to privacy issues generally, extolling the benefits of using PIAs early in the project life-cycle (interview with OFPC).

By 2007, PIAs had become mainstream in a range of Commonwealth Government agencies, including Health, the Attorney-General's Departments, the Australian Bureau of Statistics, and (with qualifications) the Department of Human Services. The Australian Government Information Management Office (AGIMO) had conducted PIAs on the succession of sub-projects conducted within the Australian Government Authentication Framework (AGAF) programme, and urged conduct of a PIA at critical points within smartcard projects. Centrelink had conducted a multi-phase PIA relating to speaker authentication. The Department of Defence had embedded PIAs within its 'Fairness and Resolution' Programme.

In the Australian States and Territories, on the other hand, progress was at glacial speeds, although examples of at least compliance checks against sets of privacy principles existed in each of Queensland (in relation to a proposed smartcard-based driver's licence), Victoria (in relation to a proposed universal student number), W.A. (in relation to a proposed whole of government employee identifier), and S.A. (in relation to personal health care data, although whether any PIAs have actually performed in not clear).

There is some degree of application in the private sector. Areas in which projects are known to the author to have been conducted include toll-roads, transport ticketing, consumer eCommerce applications and participant authentication in health records systems. Coles-Myer was reported in 2006 as having applied the IPPs to a project to produce a data warehouse relating to retail customers. Given the range of organisations and projects that are seriously privacy-invasive, however, PIAs are still not widespread in the private sector, few have been widely publicised, and the author is aware of no published reports.

Some other business process methods exist, that need to be distinguished from PIAs. Whereas the public sector uses such terms as 'compliance check', 'privacy notices', 'PIA', 'privacy management plan' and 'privacy audit', the terminology applied in the private sector includes 'privacy strategy', 'privacy management (or implementation) plan', 'privacy policy', 'privacy statement' and 'privacy review'. Guidance in relation to web-site privacy policy statements is provided for Commonwealth government agencies in AGIMO (2007), and more generally in Clarke (2005).

---

## 5. PIA Guidelines

A small number of very early sets of guidance, published between 1991 and 1998, purported to relate to PIAs, but did not have sufficient scope to be properly regarded as PIA Guidelines. The earliest document that has been located that addressed PIAs as they were defined earlier in this paper is the author's own guidance, published in short

form as Clarke (1998a) with a more extensive treatment at Clarke (1998b). The Ontario Guidelines followed soon afterwards (MBS 1999), and were the benchmark for some years.

In December 2001, the then Australian federal Privacy Commissioner, Malcolm Crompton, issued 'Guidelines for Agencies using PKI to communicate or transact with individuals' (OFPC 2001). Public Key Infrastructure (PKI) is the means whereby digital signature schemes are delivered. Guideline 3 stated that "Agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI system" (p. 29). A PIA was depicted as "a method of identifying privacy risks so that these can be highlighted and addressed when ... systems or ... business applications are being designed, implemented, revised or extended. A PIA may be part of a larger risk assessment and management procedure. Properly done, this assessment will include an understanding of which parties will bear what risks" (p. 35).

Throughout the world, the extent of implementation of PKI schemes has fallen far below the inflated expectations of the mid-to-late 1990s (Clarke 2001). On the other hand, many of the government projects involving PKI that have been conducted in Australia have taken at least some account of the OFPC's document.

In 2002, the New Zealand Privacy Commissioner published a 'Privacy Impact Assessment Handbook'. These have been influential in many countries, including Australia. The Commissioner also hosted an international symposium on PIAs in 2003.

In 2004, the Office of the Victorian Privacy Commissioner published a 'Privacy Impact Assessment Guide' (OVPC 2004). However the Australian Privacy Foundation expressed serious reservations about it, stating that "the document may be a guide for Privacy Law Compliance Audit, but not for Privacy Impact Assessment" (APF 2005, p. 2).

Work on PIA Guidelines during Crompton's period as Privacy Commissioner culminated in the release by his successor, Karen Curtis, of a draft for public consultation in 2004. It was published in final form two years later (OFPC 2006). The Guide was based on considerable research into the experiences of and guidance provided in other jurisdictions, particularly New Zealand, Canada and Ontario, and on experience within Australia.

Under the current statutory regime, the performance of a PIA is not mandatory. The Commissioner's communications with agencies and the private sector in relation to schemes that have privacy implications routinely contain segments of text along the following lines: "The Office suggests that a privacy impact assessment be undertaken as part of the further development of the proposal. The Office has released a Privacy Impact Assessment Guide for Australian Government and ACT Government agencies" (interview with OFPC).

During the first year after it was published, the Guide had attracted 23,000 hits and downloads, and it had become common for Requests for Tender for consultancy support for PIAs to explicitly require that the Guide be at least reflected, and in most cases complied with. On the other hand, PIAs are not yet performed as a matter of

course, even within Government, even for projects with significantly privacy-invasive features.

Support for the conduct of PIAs among privacy oversight bodies is substantial, however. A submission by Privacy NSW to a Committee reviewing N.S.W. legislation stated that: "We believe that PIAs are the best means by which government agencies can aim for best privacy practice as well as legislative compliance. It is our submission that ideally, a PIA would be a statutory requirement for any new Bill, regulation, or project significant enough to require Cabinet consideration" (NSWPC 2004, p. 31). No further progress has been made within NSW, but the Office's submission to the ALRC review was emphatic: "Privacy legislation should make it mandatory for all Commonwealth agencies and private organisations to provide and publish Privacy Impact Assessments (PIAs) for all new programs, policies and draft legislation which impacts on the handling of 'personal information'" (NSWPC 2007, p. 12).

The Victorian Privacy Commissioner submitted to a Senate Inquiry into DNA that "It is essential to conduct a Privacy Impact Assessment before biometrics are introduced" (OVPC 2005, p. 4). The Northern Territory Commissioner's submisson to the ALRC on the matter said that "The preferred approach would be to allow the OPC to consider the need for a privacy impact assessment, discuss the issue with the agency, and direct that an assessment be undertaken if necessary" (NTOIC 2007, p. 25).

Apart from the Commonwealth and Victoria, there is currently no guidance material published by State or Territory privacy oversight bodies (where they exist). The only guidelines issued by central agencies that have been identified are by the S.A. Departments of Health and of Families and Communities. These mandate PIAs for use in the early planning stages of projects involving personal information. The PIA Guidelines are broader than information privacy alone, but the PIA Proforma is limited to the (non-statutory) Information Privacy Principles. It is unclear whether they have been used.

In Queensland, the Privacy Unit provided repeated undertakings in 2005 and 2006 that it would shortly provide PIA guidance to agencies; but nothing has yet been forthcoming. The official position stated on the web-site is that "PIAs should be conducted whenever a program involving the collection, storage, use and / or disclosure of personal information is proposed, or where existing programs may be substantially changed. PIAs should also be conducted where legislation (or a legislative amendment) affecting personal information is proposed. It is not mandatory for Queensland government agencies to conduct PIAs, however completed PIAs provide a high level of documented assurance to stakeholders (such as other Government agencies and members of the community) that privacy issues relating to proposed programs, legislation or legislative amendments have been identified, considered and appropriately addressed".

In Western Australia, the Attorney-General has no position in relation to PIAs, and no agency exists that has a function relating to privacy oversight. No evidence was found of any Tasmanian government agency having any role to play in relation to advice on the performance of PIAs. The same applies to the A.C.T. and the Northern Territory.

## 6. Conclusions

This author argued over a decade ago that privacy had become a strategic factor for organisations (Clarke 1996). Too few corporations and government agencies listened, and one result was slow adoption-rates for both consumer eCommerce (usually referred to as 'B2C') and of eGovernment (sometimes referred to as 'G2C'). With the ongoing explosion in privacy-invasiveness (associated with insensitive applications of such technologies as data mining, CCTV, RFID tags, biometrics and DNA), public resistance is becoming even stronger and privacy disasters are occurring more frequently. This author has consequently re-visited the need for privacy to be addressed as a strategic factor (Clarke 2006b).

During the 2004-08, a succession of reviews of the operation of the federal Privacy Act has been conducted, initially by the Privacy Commissioner herself (OFPC 2005), then by a Senate Committee (SLCRC 2005), and finally by the ALRC during 2006-08 (ALRC 2007).

Recommendation 5 of the Senate Committee's Report was that "the Privacy Act be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information" (para. 7.13 ). By late 2007, the ALRC was of the view that "PIAs should be given some legislative underpinning in the Privacy Act ... by ...encouraging the preparation of PIAs and empowering the Commissioner to direct the preparation of a PIA where the Commissioner thinks a project or development is likely to have a significant impact on the handling of personal information" (specifically para. 44-70, p. 1207-08 and more generally paras. 44-43 to 44-77, pp. 1199-1210). The directions power would apply to private sector organisations as well as government agencies.

Momentum is building quickly towards widespread expectation that PIAs will be performed for all schemes that are potentially privacy-invasive. However, the incoming Rudd Labor Government's position on the matter is not yet known.

PIAs are a valuable technique for organisations that are considering initiatives that involve privacy-invasive technologies or processes. Organisations that already have privacy strategies in place find PIAs much easier and less expensive and time-consuming to perform, and the adaptations that PIAs give rise to are also much easier and less expensive and time-consuming to implement. The rationale for PIAs was originally based on public policy or 'good corporate citizienship' notions. During the last decade, the context has matured, and PIAs are now perceived as a risk management tool. In that form, PIAs are capable of addressing the needs of organisations and individuals alike.

---

## Appendix 1: PIA Exemplars in Australia

Lists of exemplars are to be found in the following sections of Appendix E within ICO (2007a):

- Appendix 2: Examples of PIAs by or for Australian Government Agencies (p. 15)

---

## Appendix 2: Recommended PIA Guidelines

The following small set of Guidelines is recommended 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 (2002), the Treasury Board Secretariat of Canada's 'PIA Guidelines: A Framework to Manage Privacy Risks'
- NZPC (2002), the New Zealand Privacy Commissioner's 'Privacy Impact Assessment Handbook'
- MBS (1999), the Ontario Management Board Secretariat's 'Privacy Impact Assessment Guidelines'

---

## Appendix 3: PIA Consultants

A small number of specialist consultants have experience in relation to the conception and conduct of PIAs. Larger 'brand name' consultancies may have also performed PIAs, but generally lack the specific exerptise. The following are those consultants who are known to the author to have the capacity. They are listed in reverse alphabetical order of consultant-surname.

Nigel Waters, Pacific Privacy Pty Ltd, Nelson Bay NSW

Mark Sneddon, Clayton Utz, Melbourne VIC

Anna Johnston, Salinger & Co, Crows Nest, NSW

Jeremy Douglas-Stewart, Privacy Law Consulting, Adelaide SA

Malcolm Crompton, Information Integrity Solutions, Chippendale NSW

Chris Connolly, Galexia, Pyrmont NSW

Roger Clarke, Xamax Consultancy Pty Ltd, Canberra ACT

---

## References

All items for which URLs are provided were most recently accessed in December 2007, unless otherwise noted.

AG (2006) " Media Release, Attorney-General, 26 August 2006, at http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2006_Third_Quarter_29_August_2006_-_Speech_-_Privacy_impact_assessment_guide_and_layered_privacy_policy_launch

AGIMO (2007) 'Privacy and Privacy Statements', Australian Government Information Management Office, current at December 2007, at http://webpublishing.agimo.gov.au/Privacy_and_Privacy_Statements

ALRC (1983) 'Report No.22: Privacy' Australian Law Reform Commission, 1983 (3 vols.)

ALRC (2007) 'Review of Australian Privacy Law', Discussion Paper 72, Australian Law Reform Commission, September 2007, at http://www.austlii.edu.au/au/other/alrc/publications/dp/72/

APC (1994) 'Australian Privacy Charter' Australian Privacy Charter Council, December 1994, at http://www.privacy.org.au/About/PrivacyCharter.html

APEC (2005) 'APEC Privacy Framework' Asia-Pacific Economic Cooperation, 2005, 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

APF (2005) 'Submission regarding 'Privacy Impact Assessments – a guide', issued in August 2004' Australian Privacy Foundation, February 2005, at http://www.privacy.org.au/Papers/OVPC-PIA-0502.rtf

APF (2007) 'Resources' Australian Privacy Foundation, Resources current at December 2007, at http://www.privacy.org.au/Resources/

Caslon (2007) 'Aust Privacy Regimes', Caslon Analytics, Resources current at December 2007, at profile.htmhttp://www.caslon.com.au/austprivacyprofile.htm

Clarke R. (1987) 'Just Another Piece of Plastic for Your Wallet: The 'Australia Card' Scheme' Prometheus 5,1 (June 1987) 29-45. Republished in Comp. & Soc. 18,1 (January 1988) 7-21, at http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html

Clarke R. (1988) 'Information Technology and Dataveillance' Commun. ACM 31,5 (May 1988) 498-512, at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html

Clarke R. (1994) 'Matches Played Under Rafferty's Rules: The Parallel Data Matching Program Is Not Only Privacy-Invasive But Economically Unjustifiable As Well' Privacy Law & Policy Reporter 1,1 (February 1994), at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperMatchPDMP.html

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

Clarke R. (1998a) 'Privacy Impact Assessments', Xamax Consultancy Pty Ltd, February 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html

Clarke R. (1998b) 'Privacy Impact Assessments' Xamax Consultancy Pty Ltd, February 1998, at http://www.xamax.com.au/DV/PIA.html

Clarke R. (2001) 'The Fundamental Inadequacies of Conventional Public Key Infrastructure' Proc. Conf. ECIS'2001, Bled, Slovenia, 27-29 June 2001, at http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html

Clarke R. (2001) 'Beyond the Alligators of 21/12/2001, There's a Public Policy Swamp' Xamax Consultancy Pty Ltd, October 2001, at http://www.anu.edu.au/people/Roger.Clarke/DV/PPSwamp.html

Clarke R. (2005) 'Privacy Statement Template' Xamax Consultancy Pty Ltd, December 2005, at http://www.anu.edu.au/people/Roger.Clarke/DV/PST.html

Clarke R. (2006a) 'What's Privacy?' Xamax Consultancy Pty Ltd, August 2006, at http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html

Clarke R. (2006b) 'Make Privacy a Strategic Factor - The Why and the How' in Cutter IT Journal 19, 11 (October 2006), at http://www.anu.edu.au/people/Roger.Clarke/DV/APBD-0609.html

Cowen Z. (1969) 'The Private Man' The Boyer Lectures, Australian Broadcasting Commission, 1969

Doyle C. & Bagaric M. (2005) 'Privacy Law in Australia' Federation Press, 2005

Flaherty D.H. (2000) 'Privacy Impact Assessments: an essential tool for data protection', October 2000, 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. Reprinted in Privacy Law & Policy Reporter 7,5 (2000) 85-90 (November 2000), at http://www.austlii.edu.au/au/journals/PLPR/2000/45.html. Revised version in Perrin S., Black H., Flaherty D.H. & Rankin T. M. (2001) 'The Personal Information Protection and Electronic Documents Act' Irwin Law, Toronto, 2001

Greenleaf G. & Nolan J. (1986) 'The Deceptive History of the Australia Card' Aust. Qtly 58,4 (Summer, 1986) 407-425

Gunning P. (2001) 'Central features of Australia's private sector privacy law' Privacy Law & Policy Reporter 7, 10 (May 2001) 189-199, at http://www.austlii.edu.au/au/journals/PLPR/2001/16.html

Hughes G. (1991) 'Data Protection Law in Australia', Law Book Company, 1991

ICCPR (1976) 'International Covenant on Civil and Political Rights' United Nations Organisation, at http://www.privacy.org/pi/intl_orgs/un/international_covenant_civil_political_rights.txt

ICO (2007a) 'Privacy Impact Assessments: International Study of their Application and Effects' Information Commissioner's Office, Wilmslow, I.K., December 2007, at http://www.ico.gov.uk/Home/about_us/research/data_protection.aspx

ICO (2007b) 'Appendix E: Jurisdictional Report for Australia' to 'Privacy Impact Assessments: International Study of their Application and Effects' Information Commissioner's Office, Wilmslow, I.K., December 2007, at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_appe_aus_2910071.pdf

ICO (2007c) 'Privacy Impact Assessment Handbook' Information Commissioner's Office, Wilmslow, I.K., December 2007, at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

Mason B. (2006) 'Privacy Without Principle: The Use and Abuse of Privacy in Australian Law and Public Policy' Australian Scholarly Publishing, 2006

MBS (1999) 'Privacy Impact Assessment Guidelines' 1999, revised 2001, Management Board Secretariat, Government of Ontario, at http://www.gov.on.ca/mbs/english/fip/pia/pia1.html

Morison W.L. (1973) 'Report on the Law of Privacy' University of Sydney, Sydney 1973

NSWPC (2004) 'Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998' Privacy NSW, 24 June 2004, at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_ppipareview.pdf/$file/sub_ppipareview.pdf#target='_blank'

NSWPC (2007) 'Submission by Privacy NSW in response to the Review of Privacy Issues Paper of the Australian Law Reform Commission' Privacy NSW, February 2007, , at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_alrc2007.pdf

NTOIC (2007) 'ALRC Review of Privacy: Submissions on Issues Paper 31', Northern Territory Information Commissioner, January 2007, at http://www.nt.gov.au/justice/infocomm/docs/ntic_sub_on_dp31.pdf

NZPC (1997) 'A Compilation of Materials in Relation to Privacy Impact Assessment' New Zealand Privacy Commissioner, 1997

NZPC (2002) 'Privacy Impact Assessment Handbook' Office of the New Zealand Privacy Commissioner, March 2002, at http://www.privacy.org.nz/privacy-impact-assessment-handbook/?highlight=PIA

OECD (1980) 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', Organisation for Economic Cooperation and Development, Paris, 1980, at http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html, accessed 3 April 1998

OFPC (2001) 'Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to Communicate or Transact with Individuals' Office of the Federal Privacy Commissioner, December 2001, at http://www.privacy.gov.au/publications/pki.doc

OFPC (2003) 'Submission to the Joint Committee of Public Accounts and Audit (JCPAA) on Management and Integrity of Electronic Information in the Commonwealth' Office

of the Federal Privacy Commissioner, January 2003, at
http://www.privacy.gov.au/publications/jcpaasubs.doc

OFPC (2005) 'Getting in on the Act: : The Review of the Private Sector Provisions of the Privacy Act 1988' Office of the Federal Privacy Commissioner, March 2005, at
http://www.privacy.gov.au/act/review/revreport.pdf

OFPC (2006) 'Privacy Impact Assessment Guide' Office of the Federal Privacy Commissioner, August 2006, at http://www.privacy.gov.au/publications/PIA06.pdf

OFPC (2007) 'State & Territory Privacy Laws' Office of the Federal Privacy Commissioner, resource current at December 2007, at
http://www.privacy.gov.au/privacy_rights/laws/index.html

OVPC (2004) 'Privacy Impact Assessments – A Guide', Office of the Victorian Privacy Commissioner, August 2004, at
http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf

OVPC (2005) 'Submission to the Commonwealth Senate Legal and Constitutional Committee on its Inquiry into the Privacy Act 1988 (Cth)' Office of the Victorian Privacy Commissioner, March 2005, at
http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/ED6E90678C836311CA2570110019833A/$FILE/Sen%20Leg%20Con%20Ctte%20sub.pdf

OVPC (2007) 'Privacy & Related Legislation in Australia' Office of the Victorian Privacy Commissioner, Resource current at December 2007, at
http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/2A43C5DD5A412761CA256FA400110051?OpenDocument

PLPR (1994-2006) 'Privacy Law & Policy Reporter', monthly journal, available from
http://www.austlii.edu.au/au/journals/PLPR/

Rule J.B. (1974) 'Private Lives and Public Surveillance: Social Control in the Computer Age' Schocken Books, 1974

Rule J.B., McAdam D., Stearns L. & Uglow D. (1980) 'The Politics of Privacy' New American Library, 1980

SA (2005) 'Privacy Compliance: Privacy Impact Assessments' Service Alberta, 2005, at
http://foip.gov.ab.ca/resources/guidelinespractices/chapter9.cfm#9.3

SADOH (2004) 'Code of Fair Information Practice' South Australian Department of Health, July 2004, at
http://www.health.sa.gov.au/DesktopModules/SSSA_Documents/LinkClick.aspx?tabid=57&mid=403&table=SSSA_Documents&field=ItemID&id=45&link=H%3a%5cTemp%5cHealth-Code-July04.pdf

SADPC (1989) 'Cabinet Administrative Instruction No. 1 of 1989: PC012 – Information Privacy Principles Instruction' South Australian Department of Premier and Cabinet, 1989, at http://www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf

SLCRC (2005) 'The real Big Brother: Inquiry into the Privacy Act 1988' Senate Legal and Constitutional References Committee, June 2005, at
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/report.pdf

Stewart B. (1996a) 'Privacy impact assessments' Privacy Law & Policy Reporter 3, 4 (July 1996) 61-64, at http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/39.html

Stewart B. (1996b) 'PIAs – an early warning system' Privacy Law & Policy Reporter 3, 7 (October/November 1996) 134-138, at http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/65.html

Stewart B. (1999) 'Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies' Privacy Law & Policy Reporter 5, 8 (February 1999) 147-149, at http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1999/8.html

Stewart B. (2001) 'Privacy Impact Assessment: Some Approaches, Issues And Examples' Proc. Conf. N.Z. Privacy Commissioner, 2001

Stewart B. (2002) 'Privacy impact assessment roundup' Privacy Law & Policy Reporter 9, 5 (October 2002) 90-91, at http://www.austlii.edu.au/au/journals/PLPR/2002/41.html

TBC (2002) 'Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks' Treasury Board of Canada Secretariat, 2002, at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp

Tucker G. (1992) 'Information privacy law in Australia' Longman Cheshire, 1992

UDHR (1948) 'Universal Declaration of Human Rights', United Nations Organisation, at http://www.un.org/Overview/rights.html

USDOC (2000) 'Safe Harbor' U.S. Department of Commerce, 2000, at http://www.export.gov/safeharbor/sh_documents.html

Warren A., Bayley R., Charlesworth A., Bennett B., Clarke R. & Oppenheim C. (2008) 'Privacy Impact Assessments: International Experience as a Basis for UK Guidance' Forthcoming, Computer Law & Security Report 24, 2 (April 2008)

Waters N. (2001) 'Privacy impact assessment - traps for the unwary' Privacy Law & Policy Reporter 7, 9 (February) 176, at http://www.austlii.edu.au/au/journals/PLPR/2001/10.html

Westin A.F. (1967) 'Privacy and Freedom' Atheneum 1967

Westin, A.F., Ed. (1971) 'Information Technology in a Democracy', Harvard University Press, Cambridge, Mass., 1971

Westin A.F. & Baker M.A. (1974) 'Databanks in a Free Society: Computers, Record-Keeping and Privacy' Quadrangle 1974

---

Acknowledgements

Parts of this paper draw on interactions with senior executives of privacy oversight bodies in all nine Australian jurisdictions during the second half of 2007. These arose in the context of a consultancy assignment conducted for the the U.K. Information

Commissioner's Office (ICO) by a team managed by Loughborough University. This resulted in an international study of laws, policies and practices relating to PIAs around the world (ICO 2007a), and a PIA Handbook (ICO 2007b).

The author greatly appreciates the permission of the Information Commissioner's Office's to reproduce relevant material arising from that Study as part of this paper. The author also gratefully acknowledges the assistance of his colleagues in the study team – Project Director Prof. Charles Oppenheim and Project Manager Adam Warren, both of Loughborough University (UK), Robin Bayley of Linden Consulting (Victoria BC, Canada), Colin Bennett of Linden Consulting and University of Victoria (Canada), and Andrew Charlesworth of the University of Bristol (UK). All evaluative comments, however, are the responsibility of the author alone.

---