Submission to the Senate Legal and Constitutional Committee re its Inquiry into the Privacy Act 1988

Roger Clarke

Version of 25 February 2005

This document is at http://www.anu.edu.au/people/Roger.Clarke/DV/SenateRevSub0502.html

---

Introduction

I have been active in relation to privacy issues since 1972, variously as information technology professional, researcher, consultant and public interest advocate. I provide a wide array of resources on the subject. I have been a Board member of the Australian Privacy Foundation since its inception in 1987, and draw attention to its submission to this Inquiry. My other major affiliations are listed at the end of this submission.

I provide below brief responses to each of the Inquiry's Terms of Reference, supported by references to papers that offer greater detail on each matter.

Term (a)(i)

*(a) the overall **effectiveness and appropriateness** of the Privacy Act 1988 as a means by which to protect the privacy of Australians, with particular reference to (i) international comparisons*

The Privacy Act was originally passed in 1988 (in relation to the public sector) and amended in 1989 (to extend it to credit reporting). In these first segments, I restrict my comments to those Parts, and defer comment on the private sector amendments until later.

The Privacy Act of 1988-89 was a long-delayed, modest, but reasonable implementation of the OECD Guidelines of 1980. An analysis of the shortfalls of the legislation compared with the OECD Guidelines is in Clarke (1989).

Because of its origins, the Act addressed technology of a past era, the 1970s. There has been no substantive review, and there have been no substantive enhancements, since that time. Meanwhile, it has been subject to continual weakening, through:

- utilisation of designed-in loopholes such as the uncontrolled and extensible nature of agencies' statements of purpose;
- administrative arrangements designed to work around the Act (such as mergers of departments and transfers of responsibility for schemes such as Pharmaceutical Benefits);
- amendments to other legislation that authorise a vast array of data collection, use and disclosure that was not authorised when the law was passed; and
- the emergence of technologies, capabilities and functions never contemplated by the consultant and small expert group that wrote the OECD Guidelines.

As a result of these depredations, if the Privacy Act is actually intended to be a means of protecting the privacy of Australian citizens, it is utterly inadequate.

An analysis of the shortfalls of the legislation in comparison with the needs of Australians at the commencement of the twenty-first century is in Clarke (2000a).

Those of the world's countries that place some value on their citizens' privacy have moved on beyond the dated and low standards of the OECD Guidelines and the Commonwealth Act. Some examples of extensions include anonymity, purpose justification, and requirements for the conduct of Privacy Impact Assessments (PIAs). See Clarke (2003a).

Term (a)(ii)

(a) the overall effectiveness and appropriateness of the Privacy Act 1988 as a means by which to protect the privacy of Australians, with particular reference to (ii) the capacity of the current legislative regime to respond to ***new and emerging technologies*** *which have implications for privacy*

The current regime contains no mechanisms whereby it can adapt or be adapted to new circumstances. It is the responsibility of the legislature to commission studies, to consider the submissions of the Privacy Commissioner and the reports of bodies such as the Law Reform Commission, and to take into account the submissions of researchers and interest groups. The Parliament has been seriously remiss in its execution of those responsibilities. It would be nice if people preparing public interest submissions to the present Inquiry were able to have confidence that their efforts would actually result in enhanced privacy protections.

The Attorney-General's Department has adopted the mantra of **'technology neutrality'** as an excuse for avoiding any need to confront the ravages wrought on laws by changes in technology. The notion of technology neutrality is intuitively appealing; but in many circumstances it fails. For example, there was no need to create laws relating to nuclear proliferation until nuclear technology came along. Similarly, constraints on aircraft breaking the sound barrier over settled areas were unnecessary while such speeds were theoretical. Moreover, regulation of such technologies was simply inconceivable until the technologies were invented. It was therefore sheer fluke if any form of regulatory constraint existed when they were first deployed.

In short, Parliament has a clear and important obligation to amend legislation, and create new legislation, to regulate powerful new technologies.

Parliament has failed that duty.

Chips have been miniaturised, and inserted into a variety of carriers, including **'smart cards' and now 'RFID tags'**. This has created all manner of new security vulnerabilities and privacy-invasions. A notable example is the naive and dangerous proposal by the Passports Office within DFAT to place enormously sensitive data into an RFID tag, including biometrics that will facilitate identity theft. There is no regulatory framework, and indeed no mechanism whereby the Parliament can be reliably informed about the nature, appropriate and inappropriate applications, impacts, implications, and necessary justification for and controls over, such complex, ill-understood and threatening technologies. Background information on smart cards is in Clarke (1998), and the privacy risks of smart cards applied to identification are addressed in Clarke (1997).

Proposals by the Government in relation to the capture and storage of **biometrics** are extraordinarily ill-informed and dangerous. They create scope for privacy invasion, identity theft and identity denial. The risks are summarised in Clarke (2001a). Proposals for a regulatory regime for biometrics are in Clarke (2003b). Further papers on biometrics are indexed in the annotated bibliography of my own papers, and my bibliography of other people's papers on the topic.

When I wrote about "**imposed physical characteristics** (e.g. dog-tags, collars, bracelets and anklets; brands and bar-codes; embedded micro-chips and transponders" in Clarke (1994), people told me that I'd been reading too much science fiction. The Terms of Reference for this Inquiry must now confront the fact that various organisations are seriously proposing that humans be demeaned through the at first voluntary, and shortly compulsory, use of the human body as a carrier for chips. These proposals are coming forward in a regulatory vacuum. The much-heralded FDA 'approval' for chip-implantation was merely a statement that the procedure does not automatically violate health care laws. The FDA is not even the arbiter of the rights of people in the U.S.A., far less the arbiter of the human rights of Australians.

The Parliament has a responsibility to proscribe all uses of chips in or closely associated with humans, and to sustain the ban until after research and public consultation have been undertaken and a suitable regulatory regime devised and implemented.

Other than expressing serious concern about their privacy impacts, I make no comment about **genetic technologies**. This is simply because the list of other threats closer to my areas of expertise has been so long that I have been unable to spend sufficient time to get to grips with it. The Australian Law Reform Commission's report made important contributions; and, like so many others before it, was ignored by the Government, and by the Parliament.

There is a long list of **additional technologies** that should also be subjected to examination. Data mining, CCTV, digital signatures, toll-roads that deny anonymous usage, pattern-recognition applied to car number-plates, caller-line identification, gross abuses of the 'white pages' database - IPND, auto-identification of telephone callers, and location and tracking of mobile phones, have all demanded attention from public interest organisations. They should all be subjected to publicly funded policy research, and then to appropriate regulation in order to rein in the privacy abuses that they embody.

Term (a)(iii)

*(a) the overall effectiveness and appropriateness of the Privacy Act 1988 as a means by which to protect the privacy of Australians, with particular reference to (iii) any **legislative changes** that may help to provide more comprehensive protection or improve the current regime in any way*

As argued earlier, the legislation is ancient, and requires substantial updating. The changes need to be even more dramatic than the cumulative changes in technology that have occurred since the late 1970s, because the law needs to 'play catch-up'. The changes required are documented in Clarke (1989), Clarke (2000a) and Clarke (2003a), and more specifically in Clarke (1997) and Clarke (2003b).

Term (b)

*(b) the effectiveness of **the Privacy Amendment (Private Sector) Act 2000** in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness*

When referring to the private sector provisions, the Government has variously used the terms 'light touch' and 'co-regulation'. The expression 'light touch' is appropriately descriptive, in that the Government has prioritised the interests of business enterprises over those of citizens, authorised business activities that the public regards as privacy breaches, and ensured that privacy regulation is nominal and cheap.

On the other hand, it is not appropriate to use the term 'co-regulatory' to describe the regime that was established by the amendments of 2000. A statement of the requirements of a genuinely co-regulatory scheme are in Clarke (1999a).

The exemptions and exceptions in the private sector provisions are so broad that the regime is appropriately described as being at best self-regulatory, more likely as non-regulatory, or simply anti-privacy. See Clarke (1999b), Clarke (2000b) and Clarke (2001b). I argued at the time that the Bill should not be passed. In December 2004, in my submission to the Privacy Commissioner in relation to her own review, I argued that the Act should be rescinded, and replaced by a genuinely privacy-protective statute. See Clarke (2004).

My detailed arguments in relation to specific aspects of the private sector provisions are in that submission, and I have accordingly provided it as an Addendum to my submission to the Committee.

Term (c)

*(c) the resourcing of the Office of the Federal Privacy Commissioner and whether current levels of **funding** and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate*

The OFPC's budget was substantially reduced by the Government in the lead-up to the passage of the Amendment Bill in 2000. That enabled the Government to be appearing to provide new resources to enable the Privacy Commissioner to perform their function. That was simply not the case. The OFPC has had its responsibilities greatly increased, and has no more resources, and possibly fewer resources, than prior to the addition of the private sector to its purview.

The Government has further depleted the OFPC's resources by imposing on it additional requirements, without providing the necessary increment in resources. The review of the private sector provisions is a current case in point. It is in any case invidious for a commissioner to be required to review her own office.

The impact of this has been that the OFPC is prevented from fulfilling its responsibilities. It conducts few audits, its replies to complaints and submissions are very slow, it is unable to respond quickly to sudden demands, and it is able to conduct very little own-volition research and investigation.

It is clear that any Government of the day will prefer not to enable the OFPC to challenge the activities of the Government, and to create hurdles for the private sector. The OFPC's privacy protection role will not be able to be performed in anything approaching the necessary manner unless resourcing is guaranteed by the Parliament.

References

Clarke R. (1989) 'The Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines', Xamax Consultancy Pty Ltd, June 1989

Clarke R. (1994) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' Info. Technology & People 7,4 (December 1994)

Clarke R. (1997) 'Chip-Based ID: Promise and Peril', for the International Conference on Privacy, Montreal, September 1997

Clarke R. (1998) 'Smart Card Technical Issues Starter Kit', for Centrelink, April 1998

Clarke R. (1999a) 'Internet Privacy Concerns Confirm the Case for Intervention', Commun. ACM, 42, 2 (February 1999) 60-67

Clarke R. (1999b) 'Submission to the Commonwealth Attorney-General, re: 'A privacy scheme for the private sector: Release of Key Provisions' of 14 December 1999' Xamax Consultancy Pty Ltd, January 2000

Clarke R. (2000a) 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' Xamax Consultancy Pty Ltd, January 2000

Clarke R. (2000b) 'Submission to the Inquiry into the Privacy Amendment (Private Sector) Bill 2000' by the Senate Legal and Constitutional Legislation Committee, September 2000

Clarke R. (2001a) 'Biometrics and Privacy' Xamax Consultancy Pty Ltd, 15 April 2001

Clarke R. (2001b) 'Beyond the Alligators of 21/12/2001, There's a Public Policy Swamp' Proc. Privacy.au, Marcus Evans Conferences, Sydney, 23-24 October 2001

Clarke R. (2003) 'Emergent Privacy Protection Principles' Xamax Consultancy Pty Ltd, 28 April 2003

Clarke R. (2003) 'Why Biometrics Must Be Banned' Extended Abstract of a Presentation to the Baker & McKenzie Cyberspace Law & Policy Centre Conference on 'State Surveillance after September 11', Sydney, 8 September 2003

Clarke R. (2004) 'Submission to the Review of the Private Sector Provisions of the Privacy Act 1988 (Cth), in particular the Issues Paper of October 2004' Xamax Consultancy Pty Ltd, November 2004

Author Affiliations

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also Visiting Professor in the Baker & McKenzie Cyberspace Law & Policy Centre at the University of N.S.W., Visiting Professor in the E-Commerce Programme at the University of Hong Kong, and Visiting Fellow in the Department of Computer Science at the Australian National University.

SUBMISSION
Review of the Private Sector Provisions of the Privacy Act 1988 (Cth), in particular the Issues Paper of October 2004

Roger Clarke **

Version of 26 November 2004

Summary

I have been active in privacy research, consultancy and advocacy since 1972. I was the primary drafter of the original N.S.W. Guidelines for the Operation of Personal Data Systems in 1977. I provided input to Justice Kirby in his role as Chair of the Expert Group that produced the 1980 OECD Guidelines. I have been a Board member of the Australian Privacy Foundation since its formation in 1987. I have provided submissions to many governmental and parliamentary enquiries. I was a member of the Data Protection Advisory Council that drafted the Victorian Information Privacy Act 2000. I have published many papers on privacy policy and privacy laws.

I draw attention to the critiques that I have written over the last 15 years in relation to:

- the inadequacies of the OECD Guidelines, in particular 1989a, 1997b, 1999a, 2000a, 2001h ss. 5-6 2003a and 2003b; and
- the inadequacies of the Privacy Act's provisions relating to the public sector, in particular 1989b, including a summary of the major deficiencies that were already apparent at that time, 1997a, 1997b, 1997d, 2000a, 2003a and 2003b.

The Terms of Reference for this review ask the Privacy Commissioner to "consider the degree to which the private sector provisions meet their objects".

There is a very wide range of ways in which the provisions are deficient in comparison with the expectations of an OECD-compliant statute. The exemptions and exceptions in relation to use and disclosure are particularly strong evidence of the provisions' anti-privacy nature. In addition, there is are considerable uncertainties about the law's scope, its interpretation, and what has to be done in order to comply with its provisions.

I have addressed the many specific problems on a number of occasions, in particular in 1996b, 1997b, 1998d, 1998g, 1998h, 2000a, 2000b, 2000c, 2000e, 2001h, 2003a and 2003b. I draw attention to the submissions of the Australian Privacy Foundation, the Australian Consumers Association, the Financial Services Consumer Policy Centre, the Consumer Credit Legal Service and Electronic Frontiers Australia, which will address these problems in detail.

I am not, however, addressing those aspects of the matter. **This submission focusses on Term (b)(ii) which requires that consideration be given to the provisions "in a way that ... recognises individuals' interests in protecting their privacy"**. I note that Term (b)(ii) uses the expression 'privacy', and does not restrict the review to 'information privacy'. The list below summarises my concerns, and provides access to additional detail in support of each point.

The private sector provisions are so seriously inadequate that amendments to them would not retrieve the situation. There is no solution other than to introduce new legislation, and

rescind the present provisions. It is untenable to revert to mere self-regulatory measures such as a standard or code. The first requirement of a replacement law is that it implement a modern interpretation of the OECD Guidelines, such as those of New Zealand and Victoria. The second requirement is that the regime be extended so that it is genuinely attuned to the needs of the Australian public in an era of enormously powerful information technologies.

I stress that my proposal does not imply great impositions on the private sector. (I draw to attention that I run a small business, am on the Boards of both companies and incorporated associations, and have earnt my living for the last decade as an eBusiness consultant). The legislation that I am arguing for would indeed proscribe some current activities in which business enterprises engage, and it would place limitations on others. But this is necessary in order to recover trust by consumers in the businesses that they deal with (2001f, 2001h s.8). In addition, the legislation can be structured as a genuinely co-regulatory scheme (1998g, 1999a, 2000b s.1), so as to involve much less uncertainty, and lower compliance costs, than arise under the present legislation.

Contents

---

1. Introduction

This document lists the most important defects of the private sector provisions of the Act from the viewpoint of the public interest in privacy. There are about 30 areas of serious shortfall that need to be addressed if Australians are to be provided with the privacy protections needed in the face of

massively privay-invasive technologies, and applications of those technologies by business enterprises. In each case, a reference is provided to a fuller explanation.

The inadequacies are presented in three groups:

- fundamental inadequacies inherent in the 'fair information practices' concept as codified in the 1980 OECD Guidelines;
- areas in which the private sector provisions fall short of the expectations created even by those Guidelines; and
- inadequacies that have emerged as a result of the enormous increase in the power of information technologies during the quarter-century since the OECD Guidelines were framed.

In the current context of government hostility to privacy protections, to propose the eradication of the many weaknesses, and the creation of significantly enhanced protections, may be seen by some people to be ambitious. On the other hand, many of the measures proposed in this document have already been implemented in laws in various jurisdictions, in some cases State laws and other Commonwealth laws. In addition, trust by Australian consumers is dependent on reasonable behaviour by business enterprises, which demonstrably will not happen without a regulatory framework.

The implementation of measures to address each of these problems must be undertaken carefully, however, so as to:

- avoid unnecessary constraints on business activities;
- ensure that compliance costs are proportionate to the privacy threats that the measures are meant to address; and
- provide transition periods to enable orderly adaptation of business systems and procedures.

---

2. Fundamental Inadequacies of FIP/OECD

This section identifies problems that are inherent in the so-called 'fair information practices' (FIP) approach codified in the OECD Guidelines of 1980. Background to FIP is provided in 2000a.

2.1 Protection for All Dimensions of Privacy

FIP generally, and the private sector provisions in particular, fail to provide protection for all dimensions of privacy. These include not only privacy of personal information, but also:

- **privacy of personal communications**, which has become an even greater cause for concern in recent years, with large numbers of ISPs handling email and shortly voice and SMS;
- **privacy of personal behaviour**, which includes manipulation of consumer behaviour, differential treatment of individuals based on abstract profiles, and abuse of personal information by the media, and which has recently come into sharper focus as a result of surreptitious photography by members of the public; and
- **privacy of the person**, which has become increasingly relevant in the context of biometrics, substance-abuse testing, body-screening and genetic screening.

These dimensions are discussed in 1997f and also in 1998d, 2000a, s. 6.10 and 2000b, and in the Australian Privacy Charter, Principles 7-9.

I am not suggesting a comprehensive privacy statute. What is necessary, however, is for the Privacy Commissioner to be empowered, required and resourced, in respect of all dimensions of privacy, to:

- conduct ongoing research;
- conduct awareness and education programs for the public, the private sector, and government

agencies; and
- conciliate disputes.

Law Reform Commissions occasionally undertake research into such matters, but their work is sporadic, and does not lead to a cumulative understanding of the issues. The delicate balancing of interests that is critical in these areas, and adaptation to changing circumstances, can only be achieved by vesting these responsibilities in a standing organisation. Morison (1973) made recommendations along these lines to the Standing Committee of Attorneys-General, and those recommendations need to be re-visited and acted upon.

2.2 Justification for Systems through PIAs

FIP generally, and the private sector provisions in particular, fail to require the provision of publicly-available justification for the following:

- privacy-invasive information systems;
- privacy-invasive purposes of information systems; and
- privacy-invasive features of information systems.

These issues are addressed most comprehensively in 2000a, s. 4.7(1)-(3), and also in 1989a, 1997a and 2003b.

It is critical to privacy protection that such an obligation exist in respect of business activities and proposals that have significant privacy implications.

The appropriate mechanism whereby this can be achieved is through the conduct of privacy impact assessments (PIAs). The technique is outlined in 1998a and 2003b, guidelines are provided in 1998b, and the historical development of the technique is presented in 2004b. I note that the Privacy Commissioner's Office has just issued draft PIA Guidelines, but I have not yet had the opportunity to review them.

The effectiveness of a PIA is heavily dependent on consultations with representatives of, and advocates for, the public interest. This is addressed most comprehensively in 1998b, and also in 2000a, s. 6.2, 2000b s. 2.

2.3 Justification for Adverse Decisions

FIP generally, and the private sector provisions in particular, fail to impose on businesses an obligation to communicate the justification for decisions adverse to the interests of a person.

This issue is addressed most comprehensively in 2000a, s. 4.7(3), and also in 1989a and 1989b.

2.4 The Public Accountability of Business Enterprises

FIP generally, and the private sector provisions in particular, fail to impose on business enterprises the requirement to establish and operate a suitable **complaints mechanism**. This is important to consumer trust generally; and quite critical in respect of activities with significant privacy implications. This issue is addressed in (2000b s.7).

Further, FIP generally, and the private sector provisions in particular, fail to impose on business enterprises the requirement to conduct privacy law and code **compliance audits**. This is important to consumer trust generally; and quite critical in respect of activities and proposals with significant privacy implications.

Telstra's first compliance audit was addressed in Haines 1996 and Greenleaf 1996. At that time, Telstra indicated its commitment to annual, independent audits. It is unclear whether Telstra has fulfilled that commitment. There is no mention of them at http://www.telstra.com.au/privacy/, none is located by means of a search on <privacy compliance auduit>, and there is no mention of 'privacy' in the company's Audit Committee Charter, at http://www.telstra.com.au/communications/shareholder/docs/audit_committee_charte.pdf.

It is also unclear whether other corporations whose systems have major privacy implication have made similar commitments, and if so whether they have fulfilled them.

2.5 Retention Limitation

The Explanatory Memorandum to the OECD Guidelines stated that " ... when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form". The Guidelines themselves, however, omit the requirement.

The private sector provisions also fail to ensure that data that has served its purpose is destroyed or de-identified. This is because NPP 4.2 permits retention while the data is needed "for any purpose for which the information may be used or disclosed under NPP 2". But, as discussed in sections 3.4, 3.5, 3.6, below, the use and disclosure provisions are so permissive that this is tantamount to approval for the data to be retained at the business enterprise's pleasure.

This issue is addressed in the retention limitation principle of the Australian Privacy Charter (APC 16).

2.6 No Disadvantage for Exercising Rights

FIP generally, and the private sector provisions in particular, fail to ensure that the exercise of privacy rights do not prejudice access to other rights or services.

This is addressed in the no disadvantage principle of the Australian Privacy Charter (APC 14), 2000a, s. 4.8, 2000b and 2003b.

---

3. Privacy Act Shortfalls Against FIP/OECD

This section identifies problems that derive from the privacy-unsympathetic manner in which the OECD Guidelines were interpreted into law in the National Privacy Principles and the amendments to the Privacy Act. Most of these problems reflect the fact that the negotiated conclusions of the 'Core Consultative Group' during 1999 were ignored, and a completely different Bill presented to the legislature.

3.1 The Universality of Privacy Protection Principles

As discussed in 1989a, the OECD considered the question of exceptions to the Principles, and concluded that they "should be as few as possible, and ... made known to the public".

Instead, as discussed in 1989b, the National Privacy Protection principles are subject to an extraordinarily wide array of exemptions and exceptions. It is vital that these exemptions and exceptions be removed, and the principles applied universally.

The widely varying circumstances of course need to be reflected, but the appropriate way to achieve this is through the manner in which th Principles are articulated, applied and interpreted, not by

simply ignoring them because they're inconvenient to business.

This issue is addressed most comprehensively in 2000a, s.4.2, and in 1997a, 1997b and 2000b ss. 3-4.

One of the many problems arising from this is the exemption of small business, which forces the clumsy re-inclusion of some categories under s.6D(4). Yet even then the re-inclusion only extends to organisations that trade in personal information. Any handling of personal information needs to be subject to controls. The objective of avoiding undue compliance costs is best achieved by means of a principle of proportionality, such that small risks incur small responsibilities, but not no responsibilities.

3.2 The Scope of 'Information'

As discussed in 1989a, the OECD Guidelines focus on 'personal data', defined as "any information relating to an identified or identifiable individual (data subject)".

As discussed in 1989b, however, the Privacy Act greatly restricts the scope, by referring not to 'personal information', but rather to 'records of personal information'. This has the effect of excluding data that is not, or not yet, in a record. It also expressly excludes information in a 'generally available publication'. Together these have substantially reduced privacy protections by exempting important and sensitive personal data from all aspects of the Act.

3.3 The Scope of 'Identified'

As discussed in 1989b, protection only exists for data about "a natural person whose identity is apparent, or can reasonably be ascertained, *from the information or opinion*" (my emphasis). The inclusion of the final phrase has the serious negative impact of denying protection for many categories of personal data where the individual can only be identified by associating that data with other data.

Pseudonymous data must be within-scope of privacy law, because it is capable of being re-associated with an individual. Only fully, permanently and reliably anonymous data should be out-of-scope.

There is also a deficiency in the definition of 'identifier', in that it is defined to not include name. This potentially enables a business enterprise to claim they have de-identified personal information even if the name is still associated with the data. This is addressed in 2000b.

3.4 Purpose as a Control

As discussed in 1989a, the OECD Guidelines envisage use of personal data only for the purposes specified, but including related purposes and subsequently specified purposes which are "not incompatible with" the original purposes.

In the Privacy Act, on the other hand, as discussed in 1989b, a system's purposes are established by the record-keeper, and there is no control on them other than that they be lawful (i.e. not unlawful). There is nothing to prevent so broad a definition of purpose that virtually any data is 'relevant'. There is no oversight over the purposes of personal data systems, and no provision for the disallowance of purposes. Yet worse, the Act fails to constrain disclosures to even these uncontrolled purposes.

This aspect of the private sector provisions falls far, far short of the expectations of a FIP/OECD scheme.

3.5 Consent as a Control

OECD Guideline 4 permits use and disclosure only if it is for the purpose of collection, by consent or under authority of law. It envisaged that legal authority would be clear and explicit.

Consent is comprehensively addressed in 2002.

The private sector provisions, specifically NPP 2.1(a), gut this intended protection by providing business enterprises with over 600 words of vaguely-expressed legal authorisations to use and disclose data prettymuch whenever they feel like it. Consent becomes essentially irrelevant in such diverse cases as direct marketing, research and statistics relevant to public health and public safety, and otherwise unlawful disclosure to law enforcement agencies without a warrant.

The most comprehensive loophole of all is the ignoring of consent where the business enterprise considers that the data subject "would reasonably expect the organisation to use or disclose the information". Consumers know full well that, under the Corporations Law, the function of corporations is to maximise profit, and that they can therefore be expected to exploit consumers and their data; so every individual "would reasonably expect" every corporation to use and disclose anything that they can get their hands on. Hence NPP 2.1(a) is nothing short of a negation of the relevance of consent to the use and disclosure of personal data.

Further, a practice has been adopted by some business enterprises that is usefully referred to as 'bundled consent': the consumer is presented with a cluster of consents which must be agreed to, without the scope for some to be agreed and others denied. This completely undermines the requirement that consent be meaningful, informed and freely-given. The characteristics of meaningful consent are comprehensively addressed in 2002.

The provisions in relation to non-consensual use and disclosure are completely anti-privacy in their effect, and require re-drafting. These serious inadequacies in the private sector provisions are having very serious consequences in the areas of tenancy, financial services and health.

3.6 Uncontrolled Secondary Purposes

The OECD Guidelines permit use of personal information for "purposes other than those specified" only in the cases of consent and legal authority.

NPP 2.1(a) elevated the previously informal concept of 'secondary purposes' to a level whereby it subtly, but devastatingly, destroyed that critical protection. The narrow category of 'sensitive information' is subject to the protection that 'secondary purposes' must be "directly related to" the primary purpose. For all other personal information, on the other hand, it is good enough for the data to be merely "related to", and by implication "indirectly related to", the primary purpose (whatever 'indirectly related to' might mean).

The second requirement, that the individual would "reasonably expect the organisation to use or disclose the information for the secondary purpose", is similarly hugely open-ended. As a result, any business enterprise can make a claim that almost any use of personal data is legitimised by this law.

This is addressed in 2000b. It is crucial that such gross undermining of what are nominally privacy protections be got off the statute book. As with the previous problem, very serious consequences arise in the areas of tenancy, financial services and health.

3.7 Justification for the Relevance of Data

The OECD Guidelines at Principle 2 require that "Personal data should be relevant to the purposes for which they are to be used". This fails the public's need in an important respect, however, in that

is does not require that business enterprises publicly justify the claim of relevance.

The private sector provisions fail on both counts. They impose on business enterprises no obligation either to ensure that data is only collected, stored and used if it is relevant, or to demonstrate that relevance.

This issue is addressed most comprehensivelyin 2000a, s. 4.7(2), and also in 1997a and 2000b.

3.8 Opt-Out Direct Marketing

It was, and still is, astonishing that a special sub-Principle, NPP 2.1(c), legitimises privacy-hostile practices of the direct marketing industry.

The separate process to address the particular direct marketing practice of spam concluded that marketing communications need to be based on consent, or 'opt-in' arrangements. The permissive 'opt-out' provisions of NPP 2.1(c) need to be replaced by the 'opt-in' standard in respect of direct marketing as a whole, including tele-marketing.

Direct marketing in general is most comprehensively addressed in 1998c, and the problems with the private sector provisions in 1998d and 2000b.

3.9 Generally Available Publications

An especially serious example of the negative impact of exemptions discussed section 3.1 is the complete absence of any protection in relation to personal information in 'generally available publications'.

One matter of extreme concern is telephone subscribers' data and the Integrated Public Number Directory (IPND). This contains locator data that is very sensitive for a proportion of the population, and reverse-sorting of the data discloses people's home addresses.

A further very serious concern is the authorisation that this anti-privacy measure provides for access by business enterprises to Electoral Roll data. That data is required, and provided, for purposes related to the conduct of elections. Its use needs to be constrained in accordance with its purpose, by removing the exemption from privacy protections.

This issue is addressed most comprehensively in 1997d, including a proposed framework, and in 1989b.

3.10 Outsourced Services

There has been a substantial loss of privacy protections as a result of the outsourcing of government data processing to private sector providers. The legislation fails to sustain the protections applicable to government data holdings when they pass to a private sector contractor.

This is addressed in 1997e and 2000b s. 9. It is completely inadequate for the very limited protections of the private sector provisions to be applied to public sector data that was collected under authority of law; and for the myths to be perpetrated that agencies actually impose terms equivalent to the IPPs on outsourcing providers through contract, and that the data subject has rights under a contract between the government and that company.

3.11 Data Sensitivity

As discussed in 1989a, the OECD Guidelines concluded that "it is probably not possible to identify a set of data which are universally regarded as being sensitive".

The private sector provisions fail to reflect the complexity of the concept of data sensitivity, and hence there are many circumstances in which sensitive data is not subject to the necessary protections. This issue is addressed most comprehensively in 2000a, s. 4.9, and in 1997a and 2000b.

Moreover, as discussed in 2000b, the authorisations for the handling of sensitive data are highly permissive, and it is unclear in what way the public is better off as a result of the provisions. They need to be replaced by obligations that actually protect the data that people actually regard as being sensitive.

3.12 Consultation by the Privacy Commissioner

The Act fails to impose on the Privacy Commissioner an obligation to conduct ongoing consultations with representatives of, and advocates for, the public interest.

Although the last five years have seen an improvement in accessibility:

- no resources are provided to assist public interest organisations in such consultations;
- their influence remains very low; and
- the Privacy Commissioner is under no obligation to sustain even the present, insufficiently effective arrangements.

This is all the more critical in view of the quite apparent satisfaction among industry associations that the Privacy Commissioner is attuned to their needs, and acts as a shield for industry against privacy-protective measures.

This is comprehensively addressed in 2000b, and in 1997a, 1998d, s.3 and 2000a, s. 6.1.

3.13 Resourcing of the Privacy Commissioner

The private sector provisions fail to ensure adequate resourcing of the Privacy Commissioner. Moreover, the Office has suffered large reductions in resourcing at the same time as it has been required to perform greatly increased functions; and additional tasks have been dictated by the government, without commensurate resources being provided.

As a result of the resource-shortfalls:

- key functions have been and continue to be under-performed;
- other responsibilities have to be compromised, or simply left unperformed, in order to release resources to perform key functions;
- the Office has extremely limited access to technical expertise in relation to the wide range of technologies that are undermining privacy;
- the Office has extremely limited access to consultancy expertise more generally; and
- little or no financial support can be provided to public interest representatives and advocates to ensure that they can effectively participate in consultations with the Privacy Commissioner, industry associations and corporations.

Of especial concern is that the Privacy Commissioner has conducted very little in the way of own-volition investigation of particular technologies and practices, and has not forced the hand of industry associations in areas that are in dire need of detailed Codes in order to establish where appropriate balance-points lie, and to provide a framework within which privacy-abusive behaviours can be reined in.

This is addressed in 2000a, s. 4.6.

3.14 Anonymity and Pseudonymity

Although anonymity is mentioned in NPP 8, the private sector provisions have failed to create an effective obligation to provide the necessary anonymous and pseudonymous services.

This has been particularly apparent in the case of consumer transportation, where toll-road operators in Melbourne and now Sydney are effectively imposing identification as a condition of use of major thoroughfares. Yet these corporations seem not to be subject to direct statements from the Privacy Commissioner to the effect that they must change their procedures in order to comply with the Privacy Act, and ensure that an anonymous alternative is readily available.

This is addressed most comprehensively in 1999b and 2000d, and in 1994f, 1997a, 2000a, ss. 6.8-6.9, 2000b and 2003b.

3.15 Multiple Use of Identifiers

The private sector provisions offer insufficient protections in relation to the multiple usage of identifiers. For example, they do not prevent business enterprises from collecting government-issued identifiers, nor do they regulate the collection, use and disclosure of identifiers issued by State Governments, especially driver's licence numbers.

Health care is another area of serious public concern about the centralisation of personal data in association with a Unique Patient Identifier (UPI), quite possibly introduced surreptitiously by means of a smartcard-based scheme.

The importance of preventing the consolidation of personal data on a small number of identifiers is addressed most comprehensively in 2000a, s. 6.5, and also in 1994f and 2003b.

3.16 Multiple Identifiers for Each Individual

On the other side of the coin, there is a need for individuals to be able to continue to use multiple identifiers in different contexts. Clearly such uses need to be subject to sanction in the event that they are used for criminal purposes such as fraud; and they are.

The availability of multiple identities is especially important to various categories of persons at risk. This is most comprehensively addressed in 2001g, and also in 2000b.

---

4. Inadequacies Arising from Post-1980 Technological Developments

The OECD Guidelines were negotiated in the context set by the technologies of the 1970s. Enormous changes have occurred since then. The nature of the changes is addressed in 1997a, 1997d, 1998g s. 2.5, 1999a, 2000a 2001h s.3 and 2003a.

The private sector provisions fail to address the greatly heightened privacy-invasiveness, and the new technological threats, that has been a feature of the 25 years since the promulgation of the OECD Guidelines in 1980. This section outlines some of the key areas in which change is required.

4.1 Identification and Authentication Tokens

The private sector provisions fail to provide individuals with control over 'their' identification and authentication tokens (such as chip-cards and digital signature keys).

This is addressed generally in 2000a, s. 6.6, and more specifically in Greenleaf & Clarke (1997c), 1998e and 2000b.

4.2 Biometrics

The private sector provisions fail to provide the necessary tight regulatory regime over the use of biometrics. This is looming as an extremely serious threat to individuals, and to trust by individuals in social and economic institutions.

This is addressed most comprehensively in 2003c, and in 1994f, 1997g, 2000a, s. 6.7, 2000b and 2001e.

4.3 Freedom From Surveillance

The private sector provisions fail to address rampant surveillance technologies, and to force corporations to achieve balance between their desires and those of individuals.

This is comprehensively addressed in 1988, 1994a, 1994c, 1999c, 2001a and 2003a, and in the freedom from surveillance principle of the Australian Privacy Charter.

4.4 Automated Decision-Making

The private sector provisions fail to impose a responsibility to ensure that an automated decision that is adverse to the interests of a consumer is subject to review by a human being before being communicated or implemented.

This is addressed in 1997a, 2000a, s. 6.3, and 2000b.

References

ACS (1990) 'Position Paper # 8 - Information Privacy Implications of Information Technology' Australian Computer Society, November 1990, at http://www.acs.org.au/president/1998/past/acspos8.htm

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

Clarke R. (1977) '**N.S.W Guidelines for the Operation of Personal Data Systems**' Government of New South Wales, 1977, at http://www.anu.edu.au/people/Roger.Clarke/DV/NSWPCGs.html

Clarke R. (1985) 'The Impact on Practitioners of **the A.L.R.C.'s Information Privacy Proposals**' Aust. Comp. J. 17,2 (May 1985)

Clarke R. (1987) 'Just Another Piece of Plastic for Your Wallet: **The Australia Card**' Prometheus 5,1 June 1987 Republished in Computers & Society 18,1 (January 1988), with an Addendum in Computers & Society 18,3 (July 1988), 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), at

http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html

Clarke R. (1989a) '**The OECD Data Protection Guidelines**: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law ' April 1989, at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperOECD.html

Clarke R. (1989b) '**The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines**' 25 June 1989, at http://www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html

Clarke R. (1991) '**The Tax File Number Scheme: A Case Study of Political Assurances and Function Creep**' Policy 7,4 (Summer 1991), at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperTFN.html

Clarke R. (1992) '**The Resistible Rise of the Australian National Personal Data System**' Software L. J. 5,1 (January 1992), at http://www.anu.edu.au/people/Roger.Clarke/DV/SLJ.html

Clarke R. (1993) '**Profiling**: A Hidden Challenge to the Regulation of Data Surveillance', Journal of Law and Information Science 4,2 (December 1993) ', at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperProfiling.html

Clarke R.A. (1994a) '**The Eras of Dataveillance**' (March 1994), at http://www.anu.edu.au/people/Roger.Clarke/DV/NotesDVEras.html

Clarke R.A. (1994b) 'Matches Played Under Rafferty's Rules: **The Parallel Data Matching Program** Is Not Only Privacy-Invasive But Economically Unjustifiable As Well' Policy 10,1 (Autumn 1994), at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperMatchPDMP.html

Clarke R. (1994c) 'The **Digital Persona** and its Application to Data Surveillance' The Information Society 10,2 (June 1994), at http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html

Clarke R. (1994d) 'Dataveillance by Governments: **The Technique of Computer Matching**' Information Technology & People 7,2 (June 1994), at http://www.anu.edu.au/people/Roger.Clarke/DV/MatchIntro.html

Clarke R. (1994e) '**Information Technology: Weapon of Authoritarianism or Tool of Democracy?**' Proc. World Congress, Int'l Fed. of Info. Processing, Hamburg, September 1994. At http://www.anu.edu.au/people/Roger.Clarke/DV/PaperAuthism.html

Clarke R. (1994f) '**Human Identification in Information Systems**: Management Challenges and Public Policy Issues', Information Technology & People 7,4 (December 1994) 6-37, at http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Clarke R. (1995) '**A Normative Regulatory Framework for Computer Matching**' Journal of Computer and Information Law XIII,4 (Summer 1995) 585-633, at http://www.anu.edu.au/people/Roger.Clarke/DV/MatchFrame.html

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

Clarke R. (1996b) '**Initial Reactions to 'Privacy Protection in the Private Sector': the Commonwealth Attorney-General's Discussion Paper of September 1996**' 17 September 1996, at http://www.anu.edu.au/people/Roger.Clarke/DV/CIthPte.html

Clarke R. (1997a) 'Flaws in the Glass; Gashes in the Fabric: **Deficiencies in the Australian Privacy-Protective Regime**' Invited Address to Symposium on 'The New Privacy Laws', Queen Victoria Ballroom, George St, Sydney, 19 February 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/Flaws.html

Clarke R. (1997b) '**Exemptions from General Principles Versus Balanced Implementation of Universal Principles**', February 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/Except.html

Clarke R. (1997d) '**Privacy and 'Public Registers**'' Proc. Conf. Data Protection and Privacy, IIR, Boulevard Hotel, Sydney, 12-13 May 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/PublicRegisters.html

Clarke R. (1997e) 'Outline of the Serious Dangers in the Commonwealth Government's Current **Outsourcing** Policy' 7 July 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/CltheOutsrcing.html

Clarke R. (1997f) '**Introduction** to Dataveillance and Information Privacy, **and Definitions of Terms**' 15 August 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Clarke R. (1997g) '**Chip-Based ID**: Promise and Peril' Invited Address to a Workshop on 'Identity cards, with or without microprocessors: Efficiency versus confidentiality', at the International Conference on Privacy, Montreal, 23-26 September 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html

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

Clarke R. (1998b) '**Privacy Impact Assessment Guidelines**' February 1998, at http://www.xamax.com.au/DV/PIA.html

Clarke R. (1998c) '**Direct Marketing** and Privacy', Proc. AIC Conf. on the Direct Distribution of Financial Services, Sydney, 24 February 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html

Clarke R. (1998d) '**Serious Flaws in the National Privacy Principles**' Privacy Law & Policy Reporter 4, 9 (March 1998), at http://www.anu.edu.au/people/Roger.Clarke/DV/NPPFlaws.html

Clarke R. (1998e) '**Public Key Infrastructure**: Position Statement' May 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/PKIPosn.html

Clarke R. (1998f) 'Information Privacy On the Internet: **Cyberspace Invades Personal Space**' Telecommunication Journal of Australia 48, 2 (May/June1998), at http://www.anu.edu.au/people/Roger.Clarke/DV/IPrivacy.html

Clarke R. (1998g) 'Submission to the **Senate** Legal and Constitutional References Committee's **Inquiry Into Privacy and the Private Sector**' 7 July 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/SLCCPte.html

Clarke R. (1998h) 'Supplementary Submission to the **Senate** Legal and Constitutional References Committee's **Inquiry Into Privacy and the Private Sector**' 5 August 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/SLCCPteSupp.html

Clarke R. (1999a) '**Internet Privacy Concerns Confirm the Case for Intervention**', Communications of the ACM 42, 2 (February 1999), at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html

Clarke R. (1999b) '**Identified, Anonymous and Pseudonymous Transactions**: The Spectrum of Choice' Proc. User Identification & Privacy Protection Conference, Stockholm, 14-15 June 1999, at http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html

Clarke R. (1999c) '**Person-Location and Person-Tracking**: Technologies, Risks and Policy Implications' Proc. 21st International Conference on Privacy and Personal Data Protection, pp.131-150, held in Hong Kong on 13-15 September 1999. Revised version published in

Information Technology & People 14, 2 (Summer 2001) 206-231, at http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html

Clarke R. (2000a) 'Beyond the OECD Guidelines: **Privacy Protection for the 21st Century**', January 2000, at http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html

Clarke R. (2000b) '**Submission to the Commonwealth Attorney-General Re: 'A privacy scheme for the private sector**: Release of Key Provisions' of 14 December 1999 ' 17 January 2000, at http://www.anu.edu.au/people/Roger.Clarke/DV/PAPSSub0001.html

Clarke R. (2000c) '**Submission to the Inquiry into the Privacy Amendment (Private Sector) Bill 2000** by the House of Representatives Legal and Constitutional Committee', 15 May 2000, at http://www.anu.edu.au/people/Roger.Clarke/DV/HoRSub2000.html

Clarke R. (2000d) 'How to Ensure That Privacy Concerns Don't Undermine **e-Transport** Investments' AIC e-Transport Conference, Melbourne, 27-28 July 2000, at http://www.anu.edu.au/people/Roger.Clarke/EC/eTP.html

Clarke R. (2000e) '**Submission to the Inquiry into the Privacy Amendment (Private Sector) Bill 2000** by the Senate Legal and Constitutional Legislation Committee', 7 September 2000, at http://www.anu.edu.au/people/Roger.Clarke/DV/SenatePBSub2000.html

Clarke R. (2001a) 'While You Were Sleeping ... **Surveillance Technologies** Arrived' Australian Quarterly 73, 1 (January-February 2001), at http://www.anu.edu.au/people/Roger.Clarke/DV/AQ2001.html

Clarke R. (2001b) 'Introducing **PITs and PETs**: Technologies Affecting Privacy 'Privacy Law & Policy Reporter 7, 9 (March 2001) 181-183, 188, at http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html

Clarke R. (2001c) 'Roger Clarke's **PITs and PETs Resources Site**' 6 April 2001, at http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETsRes.html

Clarke R. (2001d) '**P3P Re-visited**' Privacy Law & Policy Reporter 7, 10 (April 2001), at http://www.anu.edu.au/people/Roger.Clarke/DV/P3PRev.html

Clarke R. (2001e) '**Biometrics and Privacy**' 15 April 2001, at http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

Clarke R. (2001f) 'Privacy as a Means of Engendering **Trust in Cyberspace**' UNSW L. J. 7, 1 (June 2001), at http://www.anu.edu.au/people/Roger.Clarke/DV/eTrust.html

Clarke R. (2002) '**e-Consent**: A Critical Element of Trust in e-Business' Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, 17-19 June 2002, at http://www.anu.edu.au/people/Roger.Clarke/EC/eConsent.html

Clarke R. (2001g) '**Persons-at-Risk**', in 'Research Challenges in Emergent e-Health Technologies' 6 July 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/eHlthRes.html

Clarke R. (2001h) '**Beyond the Alligators of 21/12/2001, There's a Public Policy Swamp**' Privacy.au, Marcus Evans Conferences, Sydney, 23-24 October 2001, at http://www.anu.edu.au/people/Roger.Clarke/DV/PPSwamp.html

Clarke R. (2003a) '**Dataveillance - 15 Years On**' Proc. Privacy Issues Forum, N.Z. Privacy Commissioner, Wellington, 28 March 2003, at http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html

Clarke R. (2003b) '**Emergent Privacy Protection Principles**' 28 April 2003, at http://www.anu.edu.au/people/Roger.Clarke/DV/EPPP.html

Clarke R. (2003c) '**Why Biometrics Must Be Banned**' Proc. Conf. State Surveillance after September 11, Baker & McKenzie Cyberspace Law & Policy Centre Conference, Sydney, 8 September 2003, at http://www.anu.edu.au/people/Roger.Clarke/DV/Biom030908.html

Clarke R. (2004a) '**Very Black 'Little Black Books**'' 4 February 2004, at http://www.anu.edu.au/people/Roger.Clarke/DV/ContactPITs.html

Clarke R. (2004b) '**A History of Privacy Impact Assessments**' 5 February 2004, at http://www.anu.edu.au/people/Roger.Clarke/DV/PIAHist.html

Davison R.M., Clarke R., Smith H.J., Langford D. & Kuo B. (2003) 'Information Privacy in a Globally Networked Society: **Implications For I.S. Research**' Commun. Assoc. Infor. Syst. (12, 2003) 341-365, at http://www.anu.edu.au/people/Roger.Clarke/DV/cais0310.pdf

Greenleaf G. (1996) '**Telstra's First Privacy Audit: B-**' Privacy Law & Policy Reporter 3, 5 (August 1996) 97, at http://www.austlii.edu.au/au/journals/PLPR/1996/52.html

Greenleaf G.W. & Clarke R. (1997c) 'Privacy Implications of **Digital Signatures**', Proc. IBC Conf. Digital Signatures, Sydney, 12 March 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html

Haines J. (1996) '**Telstra's privacy audit**' Privacy Law & Policy Reporter 3, 4 (July 1996) 40, at http://www.austlii.edu.au/au/journals/PLPR/1996/40.html

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

Author Affiliations

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is a Visiting Professor in the Baker & McKenzie 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, and a Visiting Fellow in the Department of Computer Science at the Australian National University.

Navigation

Go to Roger's Home Page.

Go to the contents-page for this segment.

Send an email to Roger

Created: 21 November 2004

Last Amended: 26 November 2004
