Xamax Consultancy Pty Ltd

ACN: 002 360 456

78 Sidaway St Chapman ACT 2611

AUSTRALIA

Tel: +61 2 6288 1472, 6288 6916

Email: Roger.Clarke@xamax.com.au

Web: http://www.xamax.com.au/

15 May 2000

Ms C. Cornish

The Secretary

Standing Committee on Legal and Constitutional Affairs

House of Representatives

Parliament House

Canberra ACT 2600

Dear Ms Cornish

Re: Submission to Inquiry into the Privacy Amendment (Private Sector) Bill 2000

I refer to your call for submissions, and for your extension of the date of submission beyond the originally advertised date of 12 May.

I have been active in privacy research, consultancy and advocacy for close to 30 years,

and have published many papers on the topic. I attach an analysis of the key provisions of the Bill, disclosed by the Government on 14 December. A perusal of the Bill itself shows that there has been virtually no change from the Government's original intent, and hence the analysis applies to the Bill itself with minimal change. The document provides references to a substantial set of

resources which provide deeper information on many aspects of the public's expectation of the Parliament.

In summary:

- the Bill is emphatically **not** a privacy protection instrument;
- the Bill is an attempt to legitimise a vast array of privacy-invasive activities of corporations;
- the Bill is extraordinarily complex. The discovery of the intended and accidental loopholes it contains will excite lawyers for many years;
- **the Bill must be rejected**. The Government needs to submit a genuine privacy Bill that will satisfy both the expectations of the Australian public, and the nation's obligations arising from its 1984 accession to the OECD Guidelines.

Your sincerely

Roger Clarke

Director

SUBMISSION to the Commonwealth Attorney-General

Re: 'A privacy scheme for the private sector:

Release of Key Provisions' of 14 December 1999

Roger Clarke

Principal, Xamax Consultancy Pty Ltd, Canberra

Visiting Fellow, Department of Computer Science, Australian National University

Submitted Version of 17 January 2000

This document is at
http://www.anu.edu.au/people/Roger.Clarke/DV/PAPSSub0001.html

---

Abstract

The draft Bill fails to satisfy the needs of the public, because it contains large numbers of exemptions and exceptions, and legitimises many unreasonable uses of personal data. As a result, it would actually reduce privacy protections rather than enhance them. The draft Bill also fails to satisfy the needs of the private sector, because it is long and complex, and fails to encourage the confidence of consumers in their dealings with companies. The Bill needs to be very substantially revised, or withdrawn and re-written.

Contents

Introduction

The Government released on 14 December 1999 what it referred to as 'Key Provisions' of its draft Privacy Amendment (Private Sector) Bill, and requested comments by 17 January 2000.

The author of this submission has been active in privacy research, advocacy and consultancy for close to 30 years, and has published many papers on the topic, many of which are available on the web. He assisted the then Opposition in 1988, when it forced through very substantial improvements to the Privacy Bill regulating the Commonwealth public sector, and in 1989-90 he provided professional support to the Privacy Commissioner in relation to the implementation of the new law. He was also an active participant in negotiations with the Privacy Commissioner during 1997-98, during the development of the Commissioner's Principles, and was a member of the Attorney-General's 'Core Consultative Group' in 1999 which conducted negotiations in relation to the present proposal.

Following some brief background information, this document identifies a large number of deficiencies in the draft Bill. Unless these are addressed in a constructive manner, the Bill will not be worthy of support, and would in any case fail in its primary aim of recovering public confidence in the handling of personal data by companies.

Background

Privacy legislation has been called for since the beginning of the 1970s. Australia has had a clear obligation to its people to legislate privacy protections in the

private sector since it acceded to the OECD Guidelines in 1984. Successive governments have failed to fulfil that responsibility. It is high time that a government took on the responsibility of providing protections. The Government's commitment to do so, expressed in its election platform in 1995-96, and re-asserted in late 1998, was therefore very welcome.

The requirements of the primary international instrument, the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD 1980), are summarised in Clarke (1987). The inadequacies inherent in the 1980 instrument are described at Clarke (2000). The additional needs that have arisen during the last few decades are assessed at Clarke (2000).

During the period 1997-98, the then Privacy Commissioner, under instructions from the Prime Minister, prepared a set of 'National Principles for the Fair Handling of Personal Information'. A number of elements of that document do **not** enjoy support from privacy advocates. A great deal of the document, however, resulted from negotiation among relevant representatives and advocates, and had multilateral support from business and privacy interests. During 1999, further discussions were held by the Attorney-General's Department with a 'Core Consultative Group'. These also resulted in a great deal of agreement among participants, together with a small number of points of serious contention.

Self-regulation by the private sector has been demonstrated time and time again to be entirely inadequate. The alternative of 'hard', 'black-letter-law' legislation is also unattractive, because it is inevitably bureaucratic, inflexible and expensive, whereas privacy protections require balance and care, and the needs change over time. A third way exists. The features that are needed in order to implement a suitable 'co-regulatory' privacy protection regime are described in Clarke (1998 and 1999).

The comments provided below adopt the perspective that:

- privacy is a fundamental human right, and is to be very highly valued when it is balanced against other interests;
- the OECD Guidelines represent a very necessary, but far from sufficient, set of requirements;
- the many elements of a privacy regulatory framework that had been negotiated successfully among the Privacy Commissioner, representatives of industry, and privacy advocates should be respected; and
- the most effective and efficient approach to privacy protections is a 'co-regulatory' scheme involving Principles, a Privacy Commissioner with a substantial set of powers and the necessary resources, and Codes negotiated for specific industry sectors and activities.

The Inadequacies to be Addressed

This section identifies the inadequacies of the draft Bill and Principles, to the extent that they are evident from the Key Provisions document of 14 December 1999.

---

1. Inflexible Legislation Rather Than Codes

The Government's promise prior to gaining Government in 1986 was for a 'co-regulatory' arrangement. This idea would have involved a mix of legislation and codes, and action by corporations, industry associations and the Office of the Privacy Commissioner (Clarke 1998 and 1999). It would have enabled the examination of specific issues by the parties concerned about that issue, and the negotiation of a modus operandi consistent with the Principles, but appropriate to the circumstances. It would therefore have delivered practicable solutions, addressing the needs of the public, but without unduly onerous impositions on business.

The Government now uses the term 'light-touch legislation' instead. This seemed at first to have much the same connotations, but it is now apparent that the expression signals a shift away from people's needs.

The draft Bill is, in any case, anything but light-touch. In its efforts to comply with requests it appears to have received from special interest groups, the Government has added large numbers of qualifying clauses. The Principles alone, rather than providing a compressed and understandable framework like the OECD's 400 words, have blown out to over 2,500 words.

Moreover, these details have not been expressed in specific codes, addressing particular industry sectors, databases or services. Instead, they have been inserted into the principal legislation. If this responsibility had been delegated to the organisations and public interest groups concerned, subject to the purview of the Privacy Commissioner, then the various interests could have been carefully balanced, and the meanings of clauses and phrases could have been fairly precise. The inevitable result of the inappropriate approach adopted is that the draft Bill is long and complex, and contains many ambiguities that will result in unnecessary misunderstandings, suspicions and rancour.

The Bill needs to be stripped down to a genuinely co-regulatory instrument, and the specifics relevant to particular industry sectors, activities and personal data addressed in specific codes negotiated among organisations and the affected public and their representatives and advocates, under the supervision of the Privacy Commissioner.

---

2. Failure to Require Consultation and Participation

Principle 5 requires organisations to make information available about their policies and practices in relation to personal data. This is far from adequate. The following sub-sections briefly examine several aspects of the problem.

(1) Justification of Systems, Purposes and Features

At Clarke (1987), in the Australian Privacy Charter (1994, at 1), and at Clarke (2000), it was argued that an effective privacy protection regime must impose responsibility on the operator of a system to justify the need for it, for its purposes, and for its features, to some organisation with the power to reject the justification. The need has already been recognised in Australian law, in the context of data matching by government agencies.

The draft Bill contains no formal mechanism whereby an organisation can be called to account, nomatter how privacy-invasive the system, its purposes, or its features might be. With the dramatic increase that has occurred in the power of information technology, such a mechanism is now an essential feature of privacy protection legislation.

(2) Involvement of the Public in System Design

In Clarke (1992) and at Clarke (2000), it was argued that the design of 'extra-organisational' systems must reflect the requirements of the affected members of the public. To achieve this end, organisations need to consult with the relevant people, and their representatives and advocates for their interests. This is not merely a privacy concern, but is also vital to effective systems design, marketing and return on investment. The draft Bill fails to create any momentum in this direction.

(3) Involvement of the Public in the Code Preparation Process

The provisions of the Draft Bill that relate to the production of codes fail to directly impose a requirement on organisations that are preparing a code to consult with affected parties, and to reflect those parties' needs in the draft code. This was a point of substantial agreement among almost all parties that negotiated in the context of the Privacy Commissioner's NPFHPI and the Core Consultative Group; but it does not appear to be reflected in the draft Bill.

There is a very weak statement in cl.28(2)(g) that the Privacy Commissioner "may approve a privacy code" if satisfied that "members of the public have been given an adequate opportunity to comment on a draft of the code". This does not actually require organisations to give such an opportunity, does not require organisations to consult with any members of the public, let alone relevant ones, does not require organisations to take any notice whatsoever of the information provided by members of the public, and in any case does not preclude the Privacy Commissioner from approving the code anyway. An example of such an

abuse has been the abject failure of the Australian Direct Marketing Association (ADMA) to involve the affected public, representatives and advocates in the design of its unilateral and extremely unsatisfactory code.

The Draft Bill needs to be amended to require that, during the preparation of a code, and prior to its submission to the Privacy Commissioner for approval, the sponsors must consult with the public, its representatives and public interest advocates, and reflect their needs in the draft code.

(4) Involvement of the Public in the Code Approval Process

At Clarke (2000 and 2000), it is argued that consultation and participation are vital.

Cl.28(1) makes the statement that "the Commissioner may consult any person the Commissioner considers appropriate". This is completely inadequate. The Commissioner is an appointee of a government, and might in addition be captured by corporate interests. The Commissioner therefore needs to be subject to a requirement to consult, and to be required to do so with appropriate persons (such that the appropriateness is to be judged against external criteria).

Cl.28(2)(g) could be read as imposing a responsibility on the Privacy Commissioner to provide the public with "an adequate opportunity to comment on a draft of the code", unless the company or association sponsoring the code has already done so. This is most unsatisfactory, firstly because it creates the risk of seriously deficient drafts being submitted for approval, and secondly because it transfers to the Privacy Commissioner costs that belong in the private sector.

The Draft Bill needs to be amended to require that, as part of the process of considering an application to approve a code, the Privacy Commissioner must seek out and address the concerns of the affected public and their representatives and advocates.

(5) Ongoing Consultative Arrangements

Under the present Act, the Privacy Commissioner is free to maintain ongoing consultations with relevant parties. Previous Privacy Commissioners have sustained close relationships with government agencies and with representatives of business; but, as was argued at Clarke (2000), they have not shown the same enthusiasm for sustained relationships with organisations that reflect the public's interest.

An amendment is needed to require the Privacy Commissioner to maintain an ongoing relationship with the public, its representatives and public interest advocates.

(6) Conclusion

The serious deficiencies in consultative arrangements identified in this section need to be addressed if the Bill is to satisfy the requirements of the public and the private sector.

Unfortunately the Government has not set a good example in relation to consultation. During the meetings of the 'Core Consultative Group', the Government made clear that it would do whatever it wanted to, irrespective of the outcomes of that round of discussions. It appears that it has subsequently listened to, and incorporated, the requests of corporations and industry associations, but it has not involved the representatives of the public interest in those processes. The current round of comments has been referred to by the Government as 'consultation', but the Attorney-General's letter of invitation included the statement that "Government policy is settled in respect of the Bill".

The Government is not justified in using the term 'consultation' when it has, throughout, clearly signalled its unwillingness to take notice of the information and views provided by parties to the process.

---

3. Exemptions from the Protection Regime

It was argued in Clarke (1997 and 2000) that any form of exemption is a very blunt weapon, because it creates a void within which uncontrolled abuses can occur. Instead what must be striven for is balanced implementation of universal principles, reflecting the context.

The draft Bill fails this test because it creates many categories of complete exemption from the privacy protection regime (which are discussed in this section), and all manner of exceptions to the application of various principles (which are addressed in the following two sections). The complete exemptions are discussed in the following sub-sections.

(1) Existing Data

Under cl. 14, 15, existing data is exempted from Principles 1, 2, 6, 7, 8 and 10. This is very different from the outcomes of negotiations in the Core Consultative Group, which concluded that 2 (Use and Disclosure) and 6 (Access and Correction) would apply to existing data, although perhaps only after some time, e.g. 1-3 years. This is quite critical, and a serious compromise to public expectations unless changed.

(2) Enforcement Agencies

Under Definition 1, large numbers of government agencies, when acting as 'enforcement bodies', are provided with special standing under the Bill,

undermining Principle 2.1 (Use and Disclosure) and Principle 6 (Access and Correction). This is a serious compromise to public expectations.

(3) Definition of Identifier

Identifier is defined to not include name (Definition 2). This is a significant loop-hole. For example, under Principle 4.2, "An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose"; but it could now argue that the name can be left with the data, because name is not an identifier. This mis-definition could also confound the intent of cl.39.

This strange interpretation possibly arose because of a mistaken belief that Principle 7 could somehow preclude use of names by organisations. The definition of identifier needs to be changed to include name.

(4) Data Transfers Between Related Corporations

The OECD Guidelines require that use and disclosure of personal data be constrained to the specified purposes, or those additional purposes by consent or by law. The draft Bill's Principle 2 purports to implement this, but in a seriously deficient manner (see section 4.2(1), below).

Cl.22, however, would completely undermine those protections. It seeks to declare that transfers between 'related' corporations are not an interference with privacy. This is a vast and completely unacceptable compromise of privacy standards. If this Bill is to gain support, that clause has to be deleted, and the standards required by the OECD Guidelines implemented.

(5) Individual, Non-Business Acts / Personal, Family or Household Affairs

Clauses 34 and 35 exempt "acts and practices engaged in by an individual other than in the course of a business", and collection and handling "by an individual only for the purposes of, or in connection with, his or her personal, family or household affairs". The headings and text are inconsistent and unclear.

(6) Media / Journalism

Clauses 37-39 exempt "acts and practices engaged in by an organisation in the course of journalism", and enshrine the protection of journalists' sources. The expression creates the risk that this could create unintended loop-holes. It is highly desirable that, in the definition of journalism ("for the purpose of making it available to the public"), the word "sole" be inserted before the word "purpose" (cl. 37(a)).

(7) Employee Records

Clauses 40 and 41 exempt "acts and practices directly related to a current or former employment relationship and employee records". This is a completely unacceptable exemption. It is acknowledged that a considerable amount of industrial law, both statute and case, relates to this particular area; but, on the other hand, privacy in the workplace is a very serious concern.

The appropriate approach is to include employee records within the scope of the statute, and then develop a code that reflects existing law. Because of the complexity of the matter, this might require a longer delay prior to the provisions coming into force.

(8) Small Business

Clauses 42-45 appear to exempt small business organisations (with turnover of less than $1 million p.a.), provided that they do not hold any 'sensitive information'; and do not "transfer personal information about an individual to anyone else for a benefit, service or advantage". The exemption does not extend to personal data acquired from third parties.

This exemption is also a matter of concern, because many such small businesses are capable of invading privacy, and larger organisations may structure their businesses in order to take advantage of the loop-hole. It needs to be monitored closely. The Privacy Commissioner's powers of research, investigation and audit, and resources to perfom those functions, would not appear to be sufficient to perform that function. They need to be extended accordingly.

---

4. Exceptions within the Protection Regime

This section identifies inadequacies evident in the Key Provisions document. The first sub-section relates to weaknesses in the set of principles as they were prepared by the (then) Privacy Commissioner. The second sub-section deals with additional weaknesses arising from the modifications made during the drafting of the Bill.

4.1 Weaknesses in the Privacy Commissioner's Original NPFHPI

The Privacy Commissioner's National Principles for the Fair Handling of Personal Information (NPFHPI) have been used as a basis for what the Bill refers to as 'National Privacy Principles'. (This term is confusing because a set of 'Information Privacy Principles' already exists in the Privacy Act 1988, applying to the Commonwealth public sector).

The NPFHPI are to a considerable extent a conventional implementation of the OECD Guidelines; but they include several serious degradations of the standard of protection required. These were described in Clarke (1997 and 1998). The

following serious deficiencies have been carried through into the 'key provisions' document.

(1) Direct Marketing

The draft seeks to grant at Principle 2(1)(c) remarkable and entirely unacceptable freedoms to direct marketing companies. This would effectively legitimate existing privacy abuses inherent both in direct mail and in outbound tele-marketing. Outbound tele-marketing practices have become highly unpopular because they interrupt people in their home environments. Yet worse, the draft Bill authorises privacy-abusive practices in Internet marketing, which it has been clearly shown will be to the direct cost of consumers (Clarke 1998).

The wording in the draft Bill is even more complex than that in the Privacy Commissioner's version. One reason is the addition of wording relating to 'sensitive information', which make the meaning very hard to extract. In addition, the latest version has weakened even further the minimal protections that the Privacy Commissioner had specified. In 2.1(c)(iv), the words "and thereafter upon request" have been deleted, which would relieve the direct marketer of the responsibility of giving consumers the express opportunity to opt-out on each occasion that contact is made. On top of all of that, some direct marketers are already adopting the position that an opt-out 'request' only has a time-limited effect.

Unless Principle 2.1(c) is deleted, and a completely re-written code negotiated between the public and its representatives and advocates on the one hand, and the relevant associations on the other, this Bill's passage would considerably **worsen** relationships between marketers and consumers. The opt-out regime legitimised by this Principle is completely against the public's interest.

(2) Law Enforcement and National Security

The draft Bill grants remarkable and entirely unacceptable freedoms to law enforcement agencies and national security agencies. The public does not trust these agencies or their officers to operate within the law, and successive studies have demonstrated that they have good grounds not to do so. These agencies must rely on specific authorisations, not vague, open-ended invitations to breach privacy. Principle 2.1(h) has to be deleted, and any additional, specific inadequacies in existing law brought to the Parliament for approval.

A further gaping loop-hole is Principle 6.1(k), which would authorise organisations to deny subject access to personal data on the basis of a mere request by any of a long and open-ended list of 'enforcement bodies'. There is not even any requirement that the 'enforcement body' explain the nature of the "likely damage to the security of Australia" that would result, let alone the provision of a judicially authorised order that is the appropriate control over such behaviour.

The draft Bill enlarges this loop-hole yet further, by deleting the word "national" from the expression "national security", such that any body that performs any kind of 'security function' can make such a request, and thereby relieve the organisation of its responsibilities under privacy law. Principle 6.1(k) also has to be deleted.

(3) Non-Criminal Law Enforcement

The most extreme and totally unreasonable provisions in relation to law enforcement exemptions relate to "breaches of a law imposing a penalty or sanction" (2.1(h)(i)), "protection of the public revenue" (2.1(h)(iii)), and the even more vague and uncontrolled concept of "seriously improper conduct" (2.1(h)(iv)). Anything less than the deletion of these sub-clauses would represent a most serious under-valuing of the privacy interest, and a most serious privacy loop-hole for government agencies of all kinds.

These provisions are repeated in Principle 6.1(j), and need to be deleted there also.

(4) Logging

The draft fails to require logging of disclosures, except in the case of the manifold, uncontrolled law enforcement exemptions in Principle 2.1(h). It has to be extended to all exceptional instances of use and disclosure, specifically those under Principles 2.1(d), (e) and (f).

4.2 Additional Weaknesses in the 'National Privacy Principles'

This sub-section addresses several specific aspects of the draft Bill that represent substantial weakenings beyond the already unsatisfactory standards offered by the then Privacy Commissioner's NPFHPIs.

(1) Uncontrolled 'Secondary Use'

The Use and Disclosure Principle (2(1)(a)(i)) has been successively weakened by the previous Privacy Commissioner and now the Government, to the point that the latest version would have no privacy-protective value whatsoever.

The genesis of the weakness was the invention of the notion of a 'secondary use'. This was followed by the statement that a 'secondary use' need only be "related to" the 'primary use'. This was a subtle but devastating undermining of the OECD formulation, which permits usage for "purposes other than those specified" only in the cases of consent and legal authority. This is so serious a shortfall from the standards set by the OECD that it alone brings into question whether this Bill could ever gain the support of the public, or represent equivalent protections under the EU Directive.

The latest formulation in the draft Bill extends the weakening yet further. It nominally recovers some of the lost protection, by stating that secondary uses of

the specific instances of 'sensitive information' (defined in Definition 7) are to be "directly related to" the primary purpose. But is also implies that, in respect of **non**-sensitive information, an indirect relationship would be sufficient. The concept of an 'indirect relationship' is so vague that almost anything could be justified.

In short, the protections against abuse of personal data have been weakened to the point that organisations might be able to claim almost any hitherto illegitimate usages as now being within the law. If authority for any such form of secondary use remains in the Bill, it must be regarded as no more than a 'Legitimisation of Hitherto Unauthorised Abuses of Personal Data' Bill, and rejected by the Parliament and the public alike.

(2) Health

A substantial set of exceptions is created for health purposes. This arises in many places within the document, including Principles 2.1d, 2.3, 6.1, 10.2 and 10.3, Definitions 7 and 9, and cls.46-47. The inclusion of these complexities makes the Principles, and the Bill as a whole, seriously difficult for all parties to comprehend. That is precisely the reason why co-regulation and specialised codes are a superior approach.

The entire health segment should be deleted from the draft Bill, and the large amount of material considered, in its specific context, in a code under the new Act.

(3) Sensitive Information

A substantial set of exceptions is created relating to sensitive information. These arise in many places, including Principles 2.1(a), 2.1(c), 10.1 and 10.2, and Definition 7. The approach adopted has been to identify specific categories of data that are defined to be sensitive, but then to authorise widespread collection, use and disclosure of them. It is unclear in what way the public is better off as a result of these highly permissive arrangements.

Moreover, the approach fails to reflect the fact that sensitivity of personal data is highly context-dependent, and cannot be reduced to a list (Clarke 1987 and 2000). It fails to cover, for example, gender, age, personal security factors (including identity, address, employer, work-location and telephone-number), and personal data of especial sensitivity to indigenous people, such as the names of the dead. It fails, above all, to impose responsibility on the operator of a personal data system to take sensitivity of personal data into account in its handling of data and in its communications with people.

(4) Access and Correction

The rights of subject access and correction (Principle 6) have been dramatically weakened, as a result of catering to all manner of special pleadings by all manner of interests. This evidences the low value placed on privacy in the drafting of the

Bill; and creates serious doubt that this Bill makes any substantive change to the patterns that have developed in industry in relation to the handling of personal data. The multiple aspects of this devaluation are addressed in sections 5(6) to 5(9), below.

---

5. Further Specific Weaknesses in the Principles

The Key Provisions document states that "The NPPs ... have been modified in their application to 'sensitive information' and 'health information'". In fact, a great many additional changes have been made which have not been brought to the reader's attention. Many of them are editorial or draftsmanship in nature; but a significant number are substantive, and most of those further weaken the Principles' effect. It is most disconcerting that these changes were not drawn to the reader's attention.

(1) Relevance of Data to Specific Decisions

The OECD Guidelines at Principle 2 require that "Personal data should be relevant to the purposes for which they are to be used". It does not appear that there is any such requirement in the Principles in the draft Bill. (It is possible that successive drafts of Principle 2.1 may have wandered in such a manner that this fundamental requirement eventually got lost). This is so serious a shortfall that any claim that the Bill satisfies the international standard is unsustainable.

(2) Data Quality Relationship to Purpose

The OECD Guidelines at Principle 2 require that "Personal data, ... to the extent necessary for the purposes for which they are to be used, should be accurate, complete and kept up-to-date". The draft Bill's Principle 3 omits the relationship between the purposes and the quality factors. This is a serious inadequacy, because quality is a relative rather than an absolute concept. The Principle 3 needs to be amended to measure up to the OECD standard.

(3) Legitimacy of Organisations' Functions or Activities

In Principles 1.1 and 10.1(d), the word "legitimate" has been deleted from the expression "[the organisation's] legitimate functions or activities". This renders Principle 1.1 virtually meaningless, and undermines 10.1(d), because any organisation can claim almost anything to be "a function or activity", even if it is outside its constitution, or, indeed, illegal.

(4) Specificity of Authorisation

In Principles 2.1(g), 6.1(h) and 10.1(b), the word "specifically" has been deleted from the phrase "specifically authorised by or under law". This has the effect of sustaining the time-honoured ability of organisations to justify privacy-abusive

uses, disclosures and denials of subject access by reference to vaguely-worded expressions in statutes. The word "specifically" was inserted as a result of negotiation in good faith among the Privacy Commissioner, privacy advocates and business representatives. Its removal indicates the emptiness of those discussions.

(5) Availability of Organisations' Information Management Policies

The re-phrasing of Principle 5.1 has resulted in weakening of the wording that had resulted from careful negotiation with the Privacy Commissioner. The document is now only to be "available to anyone who asks for it", whereas previously the policies were to be "readily available". The requirement to "ask for it" fails to cover the increasingly prevalent context of "looking for" or "searching for" information, typically by means of menus, search-engines and entry-points on the web.

Similarly, Principle 5.2 is limited to "on request by a person", whereas the wording of the OECD Principle 6 is "means should be readily available", which contemplates access without a request. It is vital that the draft Bill be brought up to the standard required by the OECD.

(6) Inadequacies in the Access Provisions

OECD Principle 7 enables a person to obtain confirmation of whether an organisation holds data relating to them, even if access to it can be denied. The draft Bill Principle 6 provides no such right. The draft Bill needs to be upgraded to meet the standards of the OECD Guidelines.

OECD Principle 7 further provides that subject access is to be "within a reasonable time, in a reasonable manner, and in a form that is readily intelligible". The draft Bill's Principle 6 spends 400 words on exceptions to the right of access, but fails to ensure that such access that remains is subject to basic safeguards. The draft Bill needs to be upgraded to meet the standards of the OECD Guidelines.

(7) Additional Excuse to Deny Access

Principle 6.1(c) has been inserted, with the intention of permitting subject access to be refused if "providing access would have an unreasonable impact on the privacy of other individuals". This is an additional and serious compromise to the subject access principle. At the very least, it must be amended to place the onus on the information-holder to endeavour to overcome that problem, e.g. by appending "and it is not possible to provide access in such a manner as to prevent that unreasonable impact".

(8) No Review of Denials of Access

OECD Principle 7 provides for "the right ... to be able to challenge" a denial of access to personal data. The Privacy Commissioner's NPFHPI were seriously deficient in this regard, because they required review by an independent process only for denials of access to evaluative information. But even that (already highly inadequate) Principle was deleted from the expression in the draft Bill, once again without comment. Especially in view of the lack of clarity concerning sanctions and enforcement (see section 8), it is far from clear that this Principle will be replaced by an equivalent provision elsewhere in the Bill. This serious flaw has to be rectified.

(9) Inadequate Correction Rights

OECD Principle 7 provides that, "if a challenge to data is successful", then there is a right "to have the data erased, rectified, completed or amended". The draft Bill merely requires "reasonable steps to correct" the data. This fails to deal with circumstances in which the data should be deleted (e.g. because it is irrelevant to the purpose, was collected illegally, or relates to a different person entirely). The draft Bill needs to be brought up to the standard of the OECD Guidelines.

(10) Transborder Data Flows

The Privacy Commissioner's Principle 9 provided a general protection against transfers of personal data to organisations that are not subject to equivalent privacy protections. Without notice, the draft Bill has dramatically reduced the scope of the protection, by applying it only to transfer of personal information "to a foreign country". There are organisations in Australia that would not be subject to this statute if it were to be enacted, e.g. because they are created by and / or subject to State laws. The words "who is in a foreign country" need to be deleted.

Moreover, in Principle 9(f), the draft Bill has deleted the word "collected" from the NPFHPI expression. This means that the organisation no longer has an obligation to take reasonable steps to ensure that the organisation it is transferring data to will collect the data in a reasonable manner. Risks that arise from this undocumented change include misrepresentation of the organisation's purpose or functions (1.1), use of unlawful and unfair means (1.2), no effort to ensure awareness (1.3 and 1.5), and the disappearance of the obligation to collect from the individual unless it is not reasonable and practicable to do so (1.4). It is essential that the word "collected" be re-inserted.

(11) Non-Profit Organisations and Sensitive Information

Principle 10 comprises a mass of qualifications to the Collection Principle (1). The draft Bill amended, once again without any notice to the reader, Principal 10.1(d), by weakening the requirement from "not disclose without consent" to "undertake to not disclose without consent". This is an unjustifiable inadequacy,

because it relieves organisations of an obligation they should and would expect to have. The original formulation needs to be re-instated.

(12) Health Services and Sensitive Information

Principle 10.2 is a complex set of exemptions that creates enormous scope for loop-holes in privacy protection. Firstly is relates to 'sensitive information' when it should relate to 'health information' (because such matters as philosophical beliefs and trade union membership have nothing to do with health care). Secondly, it delegates to health or medical bodies the ability to make rules that must be negotiated among multiple interests, and especially privacy interests, and must remain under the purview of the Privacy Commissioner. Principles 10.2(b)(ii) and 10.3(d)(ii) need to be deleted.

(13) Absence of the 'No Disadvantage' Principle

At APC (1994 at 18), and Clarke (2000), it was argued that the exercise of privacy rights must not prejudice access to other rights or services. There appears to be no provision of that nature in the draft Bill.

---

6. Inadequate Code Approval Criteria

Cl.28(2) states that the Commissioner "may approve" a code if satisfied that a set of circumstances apply. This is a very serious weakness, because it fails to preclude the Commissioner from approving a code even if the Commissioner is not satisfied about those factors, or if the Commissioner is satisfied but should not be.

It cannot be assumed that the Commissioner will automatically act as a protector of the people, and exercise available prerogatives in a manner appropriate to a protector of the public interest. Previous Privacy Commissioners have made clear both by word and deed that they interpreted their role as being that of the administrator of a statute accountable to the Attorney-General, not a public interest watchdog accountable to Parliament. Moreover, there are serious risks of inappropriate appointments by future governments, inadequate resourcing, and capture by government agencies and / or corporations (see Clarke 2000). This fundamental weakness in the draft Bill has to be overcome.

---

7. No Compulsory Complaints-Handling Mechanism Within Organisations

It appears from Cl.28(2) that the draft Bill fails to require each organisation to establish a complaints mechanism. If so, this would be completely inadequate. It is a fundamental requirement (in the interests of organisations just as much as

individuals) that problems be addressed as close to their source as possible. This enables companies to sustain and even enhance their relationships with their customers, and avoids lengthy, costly, unpleasant, energy-sapping and attention-diverting arguments.

This inadequacy may have arisen from confusion as to whether industry associations that are instrumental in the preparation of codes should be required to have a complaints mechanism. There is more than a little doubt as to whether such mechanisms can be effective, because of the need for sanctions, and the probable inability for industry associations to impose them as a result of trade practices law. It might therefore be feasible for industry association schemes to omit complaints-handling; but it is imperative that organisations that handle personal data themselves have complaints-handling processes.

---

8. Lack of Oversight, Sanctions and Enforcement

The Privacy Commissioner must have not merely the legal capacity, but also the legal responsibility, and commensurate resources, to perform oversight functions effectively. This includes complaints-handling, research of his or her own volition, and investigations and audits of his or her own volition.

In addition, it is a fundamental requirement that any protection regime have effective back-end sanctions and enforcement mechanisms. If not, then the legislation would be worse than useless, because it would provide the appearance of action, yet it could and would be ignored by companies, because there would be no scope for legal retribution. This applies whether the corporation in question is directly subject to the Principles, or to a Code.

The material made available to date does not make clear how, or even whether, corporate behaviour will be subject to effective oversight, sanctions and enforcement. If it is not, then the Bill is worthless, and will be rejected.

---

9. Failure to Address Outsourced Government Operations

During the last few years, a great deal of government processing of personal data has been outsourced to the private sector. This has undermined the existing protections for personal data that have existed since the passage of the Privacy Act 1988 (Dixon 1997).

The Government acknowledged in 1997 that legislation was needed to ensure that these protections were not undermined. It introduced the Privacy Amendment Bill 1998 to achieve that end. The Bill lapsed when Parliament was prorogued for the most recent election. The Key Provisions document does not incorporate the changes that were in that Bill.

Public sector data is collected in many cases under compulsion, and in many cases by an agency that is a monopoly service-provider. The private sector provisions in the draft Bill are a great deal weaker than those in the existing Act. It is therefore completely inadequate for the provisions relating to the private sector to be applied to public sector data being handled by the private sector under contract to government agencies. The Bill has to be amended to incorporate the necessary additional changes, in order to sustain the existing level of protections of personal data held by governments.

---

10. Failure to Provide 21st Century Protections

In Clarke (2000), the OECD Guidelines were argued to be relevant to the technology and practices of about 1970, and to be utterly inadequate to protect people against information technology as it is used in the year 2000. The Key Provisions document falls far short of what is needed from a statute being passed at the beginning of the new millenium. Key inadequacies are as follows.

(1) Decision-Making by Artefacts

At (Clarke 2000), it was argued that the operator of a personal data system needs to ensure that all decisions about human beings (or at least those that might reasonably be expected to have negative consequences for the people concerned) are subject to review by a human being before being communicated or implemented. The EU Directive contains such a requirement. The draft Bill needs to be amended to impose this responsibility.

(2) Multiple Identifiers for Each Individual

At (Clarke 2000), it is argued that individuals are free to use different identifiers with different organisations, and when conducting distinct relationships with the same organisation. (Fraud through the abuse of identities should of course be a criminal offence, and it is). Precedents are set for this freedom by the official approval for multiple identifiers for individuals in instruments such as the Law Enforcement And National Security (Assumed Identities) Act 1998 (N.S.W.), and the Witness Protection Act 1994 (Cth). The draft Bill needs to be amended to re-affirm the availability of that protection quite generally.

(3) Identification Tokens

At (Clarke 2000), it was argued that protections are needed in relation to ID tokens generally, and particularly in relation to intrusive tokens such as id-cards that contain computer chips, and encryption keys used to electronically 'sign' messages and transactions. The draft Bill needs to be amended to provide such protections.

(4) Biometrics

At (Clarke 2000), it was argued that protections are urgently needed in relation to all uses of biometrics. In particular, it is vital to ensure that biometric measures are only ever known to a computer chip held by the individual, and to a secure device that is currently measuring the person concerned. (Such a scheme would be analogous to the mechanism that has been in use for many years to protect secure PINs that are input on ATM and EFT/POS keyboards – biometrics are effectively a PIN that can't be changed if someone else comes into possession of it). Several designs that have recently become public appear to fail that critical test. The draft Bill needs to be amended to provide such protections.

(5) Pseudonymity

The 'National Privacy Principles' include a provision relating to anonymity, which is unchanged from that in the Privacy Commissioner's formulation. At Clarke (1996, 1999 and 2000), it was argued that the additional concept of protected indirect identification, or 'pseudonymity', needs to be formally recognised. This is because it offers a means of balancing the interests of privacy and accountability. The draft Bill needs to encourage pseudonymity, by requiring legal, organisational and technical protections for the means of relating the pseudonym or persona to the person (or persons) behind it.

(6) The Scope of Privacy Protections

At (Clarke 2000), it was argued that the Privacy Commissioner's purview must extend far beyond mere data protection, to encompass all dimensions of privacy, including the privacy of the person, of personal behaviour, and of personal communications. This is important not just in its own right, but also because of the increasing interactions between data privacy and other aspects of privacy. The draft Bill needs to be amended to at least extend the Privacy Commissioner's research, public education and complaints-handling powers to all forms of privacy invasion.

Conclusions

Throughout the Key Provisions document, it appears that the Government has little interest in the public's need for privacy protection. It is as though the Government's intent were to create an image of a protective regime, while actually reducing privacy protections, and legitimising privacy-abusive practices.

Every right that the draft Bill appears to create is qualified so heavily that it actually reduces existing privacy protections. It is difficult to imagine what unreasonable practices businesses might be indulging in, or might consider introducing in the future, that would be rendered illegal, or even subjected to meaningful controls, by the Bill as it stands. To attract support from the public,

and hence to address the needs of business as well as the public, the Bill needs to be either very substantially revised, or withdrawn and re-written.

References

Clarke R. (1987) 'The Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines', 66 pp. (June 1987). At http://www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html

Clarke R. (1992) 'Extra-Organisational Systems: A Challenge to the Software Engineering Paradigm', Proc. IFIP World Congress, Madrid, September 1992, at http://www.anu.edu.au/people/Roger.Clarke/SOS/PaperExtraOrgSys.html

Clarke R. (1996) 'Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue', Conference on 'Smart Cards: The Issues', Sydney, 18 October 1996, at http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html

Clarke R. (1997) '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. (1997) '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. (1998) '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. (1998) 'Ad Code Must Respect Web Culture', The Australian, 15 December 1998, at http://www.anu.edu.au/people/Roger.Clarke/EC/ACS981215.html

Clarke R. (1999) 'Internet Privacy Concerns Confirm the Case for Intervention', Communications of the ACM, 42, 2 (February 1999) 60-67, at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html

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

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

Dixon T. (1997) 'Privacy laws: why they're a must for the public good' The Sydney Morning Herald, Tuesday April 29, 1997, p.19, at http://www.anu.edu.au/people/Roger.Clarke/DV/Outsourcing.html

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/dsti/sti/it/secur/prod/PRIV-en.HTM

Privacy Charter (1994) 'Australian Privacy Charter', Australian Privacy Charter Council, December 1994, at http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyCharter.html