A CRITIQUE OF THE AUSTRALIAN LAW REFORM COMMISSION'S INFORMATION PRIVACY PROPOSALS[1]

Graham Greenleaf[2] & Roger Clarke[3]

CONTENTS

INTRODUCTION

In April 1976 the Commonwealth Government referred the question of privacy issues arising under Commonwealth and Territorial laws to its Law Reform Commission. This paper considers those aspects of the Commission's

---

[1] This paper was presented to the 54th Australian and New Zealand Association for the Advancement of Science (ANZAAS) Congress, Section 42 (Law), held at The Australian National University, Canberra, May 14-18 1984.

[2] Lecturer in Law, University of New South Wales

[3] Reader in Information Systems, Australian National University.

Privacy Report[4], released in December 1983, dealing with what has come to be called "information privacy".[5] The Commission's Report of over 1000 pages is the most comprehensive study of privacy undertaken in Australia, and one of the most comprehensive undertaken anywhere in the world. As such, its findings and recommendations should be the "touchstone" for debate on privacy issues in Australia for at least some years to come, and may also have significant impact overseas.

The Commission's proposals are briefly outlined. The assumptions underlying them are examined and a further information Privacy Principle to deal with the "political" dimension of privacy is suggested. Reliance on freedom of information legislation as a surrogate for an "Openness Principle" is criticised. The rights of access and alteration to personal records proposed by the Commission are examined, and suggestions made for improvement. Recent developments is database technology and some problems they may cause in enforcing rights of access are raised. Methods of enforcing the other Information Privacy Principles are discussed.

2. OUTLINE OF THE COMMISSION'S PROPOSALS

2.1 INFORMATION PRIVACY PRINCIPLES

The key element in the Commission's proposals is a set of 10 Information Privacy Principles which are intended as general principles applicable to virtually all information systems. The principles[6] deal with standards for the collection and storage of personal information, the entitlement of the subject of that information to obtain access to it and to have corrections made, and controls on the use and disclosure of that information, both by the party collecting and storing it, and by third parties into whose hands it comes. "Of necessity, the principles are widely expressed and in general terms. They are statements of principle and aspiration, they are not intended to be statements of inflexible law."[7]

Because the principles are of such general application, they do not purport to provide the full extent of protection which may be necessary or desirable in some information systems. The Commission sees these more detailed specific sets of principles being developed by the proposed Privacy Commissioner or by the organizations concerned, and implemented either voluntarily[8] or as a result of subsequent legislation.[9] In addition, Clause 115(1)(b) provides for regulations to be made to ensure that records are "securely stored and are not misused", which may enable some aspects of the Principles to be implemented by regulation, possible on the advice of the Human Rights Commission.[10]

The 10 general Principles are, however, to be given legislative approval as "the basis for the protection of privacy in the information processing

---

[4] Australian Law Reform Commission Privacy Report No. 22, 3 Vols (Vol 3 microfiche only), Australian Government Publishing Service (AGPS), Canberra, 1983. The Report is referred to hereinafter as "ALRC22". References in square brackets "[ ]" are to paragraph numbers of the reports.

[5] The Report also deals with many aspects of privacy which are not necessarily related to information systems, such as intrusive conduct and physical surveillance.

[6] Reproduced in Table 1

[7] ALRC22 [1200]

[8] ALRC22 [1054]

[9] ALRC22 [1415, 1418]

[10] ALRC22 [1399, 1402]; discussed in 7.1 below

context"[11], by virtue of their inclusion as Part II of the Schedule to the Draft Privacy Bill 1983[12] recommended by the Commission. This is to indicate Parliament's approval of the principles as a "guide to proper information-processing practices."[13] The Commission notes that "this is a novel approach to implementing general principles in Australian law".[14]

"Privacy" is not defined in the Draft Bill, in keeping with overseas privacy legislation.[15]

> "For the purposes of this Act and of any other enactment, where a person does an act, or acts in accordance with a practice, that is contrary to or inconsistent with anything set out in the Schedule, the act or practice shall be taken to be an interference with the privacy of a person."

The failure of an organisation to comply with the Principles will be therefore sufficient to give the Privacy Commissioner jurisdiction to inquire into a complaint of interference with privacy.[16] The powers of the Human Rights Commission are expanded analogously.[17]

2.2 PRIVACY COMMISSIONER

The Commission recommends that there be a Privacy Commissioner who is a full-time member of the Human Rights Commission.[18] Some of the functions of a "statutory guardian" of privacy would rest with the Human Rights Commission as a whole, including the function of making recommendations to Government and other bodies on privacy issues generally.[19] Other functions, including that of inquiring into and making recommendations concerning particular complaints,[20] are to be exercised by the Privacy Commissioner. The provisions of the Draft Bill appear to allow the Human Rights Commission and the Privacy Commissioner to decide, as a matter of administrative practicality, the boundaries between general and particular inquiries.[21] The powers of the Privacy Commissioner and the Human Rights Commission in relation to privacy are, in general, similar, but the power to issue binding and enforceable orders concerning access to and correction of records is exercised by the Commissioner alone.[22]

2.3 RIGHTS OF ACCESS AND CORRECTION

Two of the Information Privacy Principles, those concerning access to and correction of records, are to be made enforceable by individuals against record-keepers.[23]

---

[11] ALRC22 [1200]
[12] Hereinafter "Draft Bill"; all references to "Clauses" are to Clauses of the Draft Bill.
[13] Ibid
[14] Ibid
[15] ALRC22 [19,594]
[16] Draft Privacy Bill 1983, ALRC22 Vol.2 pg.211 (hereafter "Clauses"), Clauses 12,21
[17] Clause 10(2)
[18] Clause 11
[19] Clause 10(1)
[20] Clauses 7, 12, 21
[21] Clauses 10(2), 12
[22] Clause 92
[23] Clauses 51, 68

A person's right of access to a record of personal information is subject to a number of exemptions, most of which are based on the exemptions for access to documents under the Freedom of Information Act 1982 (Cth), and have been adopted because of what the Commission sees as a "need for harmony" with that Act.[24]

By Clause 68 "A person who considers that a record of personal information about him consists of or includes information that is inaccurate, out-of-date, misleading, incomplete or irrelevant" may request the record-keeper to make the appropriate alterations to the record. In determining whether an alteration is required on one of these grounds, the purpose for which the information "was obtained or is being kept by the record-keeper shall be taken into account".[25]

If a record-keeper does not comply with a request for access or alteration, the person has a right to apply to the Privacy Commissioner for a direction to the record-keeper to provide access or alteration as requested or as otherwise specified.[26] A right of appeal lies from the Privacy Commissioner to the Administrative Appeals Tribunal.[27] There is also an option of first applying for an internal review of decisions made by public sector record-keepers.[28]

The right of alteration is to replace the more limited right found in Part V of the Freedom of Information Act 1982 which was only intended as an interim measure.[29]

2.4 SCOPE OF THE PROPOSALS

One of the most notable features of the Commission's proposals, in contrast to the legislation in many other countries, is that they are intended to apply to both public and private sector record-keepers.[30] The proposals also apply to both automated and manual record-systems.[31] Comparable legislation in the United States and Canada only applies to public sector record-keepers. In France and some other European countries, comparable legislation only applies to automated information systems.[32]

Due to the constitutional limitations of the Commonwealth, and the terms of the Commission's Reference, the Commission's recommendations do not apply to all records of personal information concerning Australian citizens or residents.[33] The proposals apply to all Commonwealth public sector bodies, but not to State public sector bodies. The proposals apply to the Territories.[34]

The Commission intends its proposals to apply to all private sector record-keepers, subject to the limitations noted above. They apply to "records of personal information" that are in the Australian Capital Territory or the Jervis

---

[24] ALRC22 [1253]
[25] Clause 68(4)
[26] Clause 92
[27] Clauses 91, 92(7)
[28] Clauses 90, 91
[29] ALRC22 [1279]
[30] ALRC22 [1051, 1239]
[31] ALRC22 [1193, 1413, 1415]
[32] See ALRC22 Volume 3 Appendix D "Overseas Information Privacy Laws" for a convenient compilation.
[33] ALRC22 [7-10, 1036-7, 1396]
[34] For this purpose, the Northern Territory and Norfolk Island, as self-governing Territories, are treated as States: ALRC22 [1037]

Bay Territory.[35] They also apply to records elsewhere in Australia about residents of these Territories,[36] and to records not in Australia about persons who ordinarily reside in Australia provided they are under the control of an Australian record-keeper.[37] They apply to persons who "ordinarily reside" in Australia, which would appear to exclude not only most foreigners but also some Australian expatriates.[38] Many private sector record-keepers outside these Territories will therefore come within the scope of the Draft Bill, at least insofar as some of their records are concerned.

The Commission notes that

> "It is, however, extremely important that the principles of privacy protection be the same in both the Federal and State jurisdictions ... Business and industry are particularly concerned at the prospect of significantly different approaches to privacy protection in the various jurisdictions of Australia".[39]

In tabling the Commission's Report the Attorney-General noted the Commission's call for uniformity and said that he would bring the matter to the attention of the Territories and the States.[40]

Clause 10(2) provides an unrelated but significant extension, by empowering the Human Rights Commission to inquire into any acts and practices "whether in a Territory or not, by means of or in the use of a postal, telegraphic, telephonic or other like service" which interfere with privacy. It would seem that many of the activities of private sector record-keepers throughout Australia would come within this provision. The Commission gives the examples of "direct marketing through telephones" and "direct mail".[41]

2.5 APPROACHES REJECTED OR DEFERRED

It is useful to note some alternative or supplementary approaches which were rejected by the Commission, so as to better appreciate the proposals made.

(i) Licensing: Licensing of some record systems is the basis of French law and that of the Scandinavian countries. The Commission was not convinced that information problems had reached a stage in Australia which would justify the sweeping controls normally associated with licensing, particularly the power to refuse to grant or renew licenses.[42]

(ii) Public Listing: Although the Commission saw "considerable value" in the public listing of personal record systems and their uses, as is required in the laws of the United Kingdom, United States and Canada, it did not consider that this should be required by law beyond the present requirements of the Freedom of Information Act 1982.[43]

(iii) A General Tort: The option of a general tort of invasion of privacy, or "creating a right to claim damages in respect of any 'interference with

---

[35] Clause 45
[36] Clause 46(1)
[37] Clause 46(2)
[38] Clause 45, 46
[39] ALRC22 [1393; see also 1088-92]
[40] Press Release 184/83, Commonwealth Attorney-General, dated 14/12/83
[41] Note to Clause 10
[42] ALRC22 [1202-1206]
[43] ALRC22 [1207-1208]; discussed in 4 below

privacy'",[44] was rejected as "too vague and nebulous",[45] although the Commission adheres to its 1979 recommendation "that a new statutory tort regarding publication of sensitive facts be established".[46]

(iv) Damages for Breach of Standards: A more limited remedy in damages which would "only be available where some specific privacy standard had been breached"[47] was also rejected as inappropriate to "all breaches of privacy standards", as some will be very general and not intended to be of binding authority.[48] It is clear that the Commission would not see breaches of the Information Privacy Principles as actions which should lead to a remedy in damages.

(v) Notification of Adverse Decisions: "A general requirement, whenever an adverse decision was made, to notify the person affected and to inform him of his rights" was rejected as unnecessarily costly.[49]

(vi) Logging: The desirability of requiring record-keepers to log all uses and disclosures of personal information was rejected as "not warranted by the present dangers of inappropriate access or improper disclosure". The possibility of logging being required in particular areas by use of the regulations power in the Draft Bill is noted.[50]

3 THE PROPOSALS IN CONTEXT

3.1 THE EMERGENCE OF INFORMATION PRIVACY PRINCIPLES

In explaining the influence of previous formulations of information privacy principles on its recommendations, the Commission states:

> "The most significant formulations are the guidelines recommended by the Council of the Organisation for Economics Co-operation and Development (OECD) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Convention). In Australia, the New South Wales Privacy Committee (NSWPC) has prepared draft guidelines relating to information-processing practices. These and other attempts suggest that there are a number of fundamental themes that underlie all statements of information privacy principles. These themes can be made explicit. The Commission, drawing primarily on the OECD guidelines, has formulated [the 10 Information Privacy Principles]",[51]

The OECD guidelines, which were adopted by the Council of the OECD in 1980, arose at the end of "the privacy decade of law reform and legislative activity".[52] The extent to which the OECD guidelines reflect the information privacy laws of Europe and North America enacted during the 1970's, and the numerous reports of inquiries during that decade, is catalogued by the

---

[44] ALRC22 [1075]
[45] ALRC22 [1081]
[46] See ALRC22 [1085] footnote 129, and ALRC11 Unfair Publications: Defamation and Privacy, AGPS, Canberra, 1979
[47] ALRC22 [1082]
[48] ALRC22 [1085]; discussed in 7.2 below
[49] ALRC22 [1397]; discussed in 7.4 below
[50] ALRC22 [1402]
[51] ALRC22 [1195]
[52] ALRC22 [648]

Commission.[53] The Commission's Information Privacy Principles may therefore be seen as part of what the Commission calls an "emerging pattern" concerning information privacy[54] and not only as based on the OECD guidelines. We will now examine some assumptions underlying that "emerging pattern".

3.2 THE EFFICIENCY CRITERION FOR INFORMATION PRIVACY

In a study of the growth of information privacy policies in the United States published in 1980, James Rule and others concluded[55] that Alan Westin's writings on privacy, and particularly his 1967 book *Privacy and Freedom*,[56] "have shaped virtually all current thinking about privacy as a public issue", and represent the start of a nearly unbroken consensus of official responses to the issue of information privacy, commencing with the Fair Credit Reporting Act 1970 and continuing to the Report of the Privacy Protection Study Commission of 1977.[57]

Rule characterises this "official response" or "emergent consensus" as follows:

> "... no frontal collision has occurred between an aroused public opinion and organizations engaged in what we term surveillance [... the systematic monitoring of personal data ...(used) ... in a neutral sense to indicate monitoring for all sorts of purposes, both helpful and coercive.[58]] The emergent official interpretation of 'privacy protection' has forestalled any such confrontation. In this view, the drawbacks of surveillance systems are not inherent in their nature, but lie in their failure to work 'correctly'. And 'correctly' in this context means 'efficiently' from the standpoint of the long-term interests of the organization.[59]
>
> By this ['efficiency'] criterion, surveillance is considered acceptable provided that four conditions are met: first, that personal data are kept accurate, complete and up-to-date; second, that openly promulgated rules of 'due process' govern the workings of data systems, including the decision-making based on the data; third, that organizations collect and

---

[53] ALRC22 [603] The earliest legislation and reports containing influential sets of principles were the U.S. Fair Credit Reporting Act 1970, the 1973 Report of the U.S. Department of Health, Education and Welfare Records Computers and the Rights of Citizens, Sweden's Data Act 1973, and the U.S. Privacy Act 1974. Parts of the New South Wales Privacy Committee's Guidelines for the Operation of Personal Data Systems (Background Paper 31, the Committee, Sydney, 1977; hereinafter "NSWPC Guidelines") of 1977 were clearly influenced by these early models, and their similarity in content to the OECD guidelines, noted by the Commission at [638] is therefore not surprising.

[54] ALRC22 [586]

[55] James Rule et al. The Politics of Privacy, Elsevier, New York, 1980 p.73, hereinafter "Rule"

[56] New York, Atheneum, 1967

[57] Personal Privacy in an Information Society, Govt. Printer, Washington, 1977

[58] Rule, p.47

[59] Rule, p.69

> use personal data only as necessary to attain 'legitimate' organizational goals; fourth, that the people described in data files have the right to monitor and contest adherence to those principles. By these criteria, organizations can claim to protect the privacy of those with whom they deal, even as they demand more and more data from them and accumulate ever more power over their lives. From the standpoint of surveillance organisations, this is a most opportune interpretation of 'privacy protection'."[60]

The reasons put forward by Rule for the further limitation of surveillance "as a bad thing in itself" even if it is "efficient" can be summarized as:

(i) Most people have an "aesthetic" objection to living "in a world where every previously private moment becomes a subject of bureaucratic scrutiny"[61];

(ii) There is value in "preserving what one might term a desirable 'looseness' in social relations." "[M]any if not most surveillance systems work to make people responsible for their pasts ... but most people probably feel that there ought to be limits to the extent that people's 'records' are held against them".[62] Rule considers that there is no "natural limit" to the extension of surveillance, but that an alternative must be found as a matter of conscious social policy "for organizations to relax the discriminations which they seek to make in their treatment of people". "We propose a reallocation of resources toward less discriminatory, less 'information-intensive' ways of dealing with people".[63]

The argument here is that there is no factor constraining the amount of information which the operators of information systems will seek to utilize, given the technological and organizational capacity to do so. Our society is progressing by a bureaucratic imperative (if not a technological one), to one in which decisions about individuals become progressively more "information intensive" ("discriminations" become more "fine-grained"). The question is whether this is the type of society we want, or should we limit the information available to decision-makers, recognising that in doing so we are limiting the "efficiency" of their decisions?

(iii) The most important reason, however, is "the potential of these systems for fostering excessive concentrations of power in society ... For surveillance makes it possible for those at the centres to monitor the activities of large populations and 'reach out' with forceful actions to shape and control those behaviours. ... We must remember that the purposes governing the use of surveillance systems can only be the purposes of those who control them at a particular point ... At some point, in other words, the repressive potential of even the most humane systems must make them unacceptable."[64]

Rule is arguing that there are some types of information systems that could be so dangerous that they should never be developed (or, if already existing, should be dismantled). A system may be used repressively even though used with perfect privacy "efficiency". In some cases this may be because the purpose of the system is inherently repressive. However, in other cases the original purpose of the system might be socially beneficial, but the danger arises from the possibility of use for purposes for which the system was not originally intended.

---

[60] Rule, p.71
[61] Rule, p.117
[62] Rule, p.118
[63] Rule, p.154
[64] Rule, pp.119-120

Rule's conclusion is that this possibility has received almost no consideration in the official development of privacy policy in the United States. For example, the Privacy Protection Study Commission gave no consideration to the abandonment of the Parent Locator Service "as a method of surveillance and control not worth its price in intrusion".[65] A number of examples, hypothetical and actual, are considered by Rule.[66]

One consequence of acceptance of the "efficiency criterion" is, in Rule's view, that it serves to legitimize increasing surveillance, and undercut the basis of popular opposition to it. Provided that the surveillance is carried out "efficiently", the organization concerned can claim that it is protecting privacy.[67] The American credit-reporting industry "having operated, with increasing nervousness over the years, in a kind of legal vacuum", found itself obtaining through the Fair Credit Reporting Act 1970 "something close to official endorsement of its activities ... at the price of a few quite moderate reforms".[68] It should be noted that, once it is accepted that a system should exist, Rule does not doubt that "privacy efficiency" is entirely desirable and necessary to minimize injustice.

Rule's approach provides a valuable perspective through which the Commission's proposals may be viewed as a whole, before attention is shifted to the merits of particular proposals.

3.3 THE COMMISSION'S CRITERIA FOR PRIVACY PROTECTION

In its discussion of the justifications for privacy protection,[69] the Commission canvasses a wide range of possible justifications, but seems to support four principal reasons:

(i) "[A] society in which there is total lack of respect for privacy" is rejected "as completely intolerable", arguably on grounds of human psychological need, but this may well be the same as Rule's "aesthetic" grounds.[70]

(ii) The likelihood of "grave injustices to individuals, particularly as the result of misuse of information" is seen as a practical reason for strengthening protection.[71]

---

[65] Rule, p.110

[66] The most drastic example of a change in the purpose of an information system is the use of Dutch population records during the Nazi occupation to identify and track down Jews. The near-successful attempt of the Nixon White House to use the Internal Revenue Service as a means of harassment of dissidents is a more contemporary example. The current development of electronic funds transfer systems (EFTS) has the potential, a group of experts concluded, to be the ideal unobtrusive surveillance system for an authoritarian state. Finally, the hypothetical example of a medical surveillance system designed to provide timely intelligence on threats to people's health by virtue of a tiny monitoring transmitter connected to a central computer could certainly provide many benefits, but would we risk its creation even if it was operated with "private efficiency"? (Rule pp.145-150)

[67] Rule, p.72

[68] Rule, p.92

[69] Principally in ALRC22 [32-44]

[70] ALRC22 [35], following McCloskey

[71] ALRC22 [36]

(iii) A human right of respect for individual autonomy is a further basis. "The claim to privacy is part of the general claim to protection of human rights."[72] "Basic to all the human rights identified in the ICCPR[73] and other international human rights instruments is respect for individual autonomy. Claims to privacy are part of the claim that the autonomy of each individual should be protected and his integrity respected."[74]

(iv) The "political basis of privacy protection" is also stressed: "If privacy protection were not strengthened, it would be difficult for Australian society to maintain its traditions of individual liberty and democratic institutions in the face of technological change, which has given to public and private authorities the power to do what a combination of physical and socio-legal restraints have traditionally denied to them. Privacy protections might be seen as a safeguard against political oppression."[75]

The Commission considers the development of electronic funds transfer systems (EFTS) as an example of new technology which "would no doubt make it easier for authoritarian control of society – provided that other factors were present".[76]

The "political basis" identified by the Commission would seem to justify restrictions on the development of "surveillance" beyond considerations of "efficiency" but, at least so far as information privacy is concerned, this "political basis" is not clearly addressed in the rest of the Commission's Report. Instead, when the basis of privacy protection needed because of the "information boom" is again addressed,[77] it is the "efficiency criterion" which provides the basis for the legal response:

> "It is not too late ... to attempt to control and guide the way in which organizations ... use the new information technology: in particular, through insistence that appropriate standards be observed controlling information collection, use, access and storage.[78]
>
> The individual's key concerns are to see what is recorded by people whose decision-making might affect him, and to know which other people, beyond the original record-keeper of personal information, may use it."[79] (emphasis added)

Is this only a matter of emphasis and wording, or does it have consequences for the Commission's specific proposals? When dealing with a Report of over 1000 pages, it is easy to be unfairly selective with quotations. We will now examine the specific proposals.

---

[72] ALRC22 [1032]
[73] International Covenant on Civil and Political Rights
[74] ALRC22 [1033] (see also [1193], [1230])
[75] ALRC22 [38]
[76] ALRC22 [41]
[77] ALRC22 [583-585]
[78] ALRC22 [583]
[79] ALRC22 [585]

3.4 IMPLEMENTING THE COMMISSION'S CRITERIA: THE PRINCIPLES

The 10 Information Privacy Principles are, of course, largely concerned with ensuring the "privacy efficiency" of information systems, but do they recognise wider criteria? Do they implement criteria outside that of "privacy efficiency" or encourage further consideration and implementation of such criteria?

Some of the Principles establish standards which are only to be measured in terms of the purposes of the system (which are, of course, the purposes of the system operators), and are therefore purely "internal" or "efficiency" criteria. This is explicit in Principles 3,6 and 9, which provide that assessments of whether information is irrelevant, out-of-date, incomplete, excessively personal, misleading, accurate, complete or up-to-date are to be made "having regard to the purposes of collection" or "having regard to the purpose for which the information is being used". For example, there is therefore no recognition in these principles that it may be socially desirable for old information about a person to be disregarded in the making of decisions about that person even though the system operator can demonstrate some statistical or other predictive validity in its use; it will still not be out-of-date "having regard to the purpose of collection". The individual's rights to be informed of the purposes of collection, and to obtain access to and correction of information (Principles 2,5 and 6) are also essentially "internal" matters.

It seems, too, that an assessment could only be made of whether information had been collected "unnecessarily" under Principle 1 in terms of the "purpose of collection". Similar considerations apply to Principle 7, that "personal information should not be used except for a purpose to which it is relevant". In the absence of any other Principle limiting the purposes for which systems can be established (and, therefore, information collected), no other standard is possible.[80]

It is not possible to infer from these Principles any limit on how broadly a record-keeper may define the purposes of the system. The possibility is therefore left open of so broad an initial definition of purpose that vast amounts of information are "relevant". For example, the creation of one central bureau for the purpose[81] of gaining a complete picture of a person's socio-economic history by recording credit, tenancy, employment, medical insurance details would not seem contrary to these Principles.

The Principles do not attempt to impose any absolute prohibitions on collecting or using any classes of particularly "excessively personal" information (eg on race or sexual preferences)[82], merely limiting its collection "having regard to the purpose of collection"[83]. If a purpose of collection was to discriminate against aborigines, or homosexuals, there would therefore be no breach.

On the other hand, prohibiting collection of information by "unfair" means (Principle 1) involves the imposition of standards which do not seem to be determined by the "purpose of collection" or the purpose of the system as a whole. Standards of security (Principle 4) could also be regarded as external standards.

---

[80] See 3.6 below for discussion of such a "social justification" Principle.
[81] This assumes that such a functional approach is a legitimate way to define "purpose". A "decision-orientated" approach might assert that there were multiple purposes for the creation of such a bureau. The Report gives no assistance.
[82] ALRC22 [1218-1220]
[83] Principle 3

For most information systems, adherence to these standards will also be a matter of "internal efficiency"

More important "external" standards are imposed by Principles 8 and 10, which provide that both the use of information by the original collector for purposes other than the purpose of collection, and the disclosure of that information to any third parties, are illegitimate except on three grounds: consent of the record-subject; threats to life or health; or as required by law. It is important to realize that what these Principles do is to "freeze" the legitimate operations of information systems at the point of collection of information, by assessing the legitimacy of uses of information in terms of the purpose of collection. Because of the difficulty of obtaining the consent of every existing record-subject to a new use of previously collected information in practice, further wholesale extensions of the use of information for other purposes would have to be "as required by law". In the absence of any laws giving general approval to such changes, any such change would require specific legislative approval before implementation. In effect, system operators are prohibited from changing their purposes for holding information as they go along: the standard of legitimate change is external, not internal.

The requirement that information "is not misused" (Principle 4) seems to refer to these standards in Principles 8 and 10.

It is significant that in its phrasing of principles 8 and 10 the Commission has avoided the approach of the U.S. Privacy Act 1974, which places no limits on routine internal uses of information by an agency once it has collected it, and allows disclosure to other agencies in connection with "routine uses" for purposes "compatible with the purposes for which it was collected" and to law-enforcement agencies.[84] This allows a constantly changing standard of "privacy efficiency"

The Commission recognises that all instances of "matching" ("the technique of comparing the whole or part of one set of personal records with the whole or a part of another set"[85]) will be inconsistent with these principles, unless the matching is "as required by law". The Auditor-General's argument that the whole of the Commonwealth government should be regarded as "one monolithic record keeper", allowing unrestricted matching, was rightly rejected by the Commission.[86]

3.5 IMPLEMENTING THE COMMISSION'S CRITERIA THE DRAFT BILL

The Privacy Commissioner may receive a complaint under Clause 12 that the practice of maintaining a particular information system was an interference with a person's privacy because of the severity of the risks involved in the potential misuse of the system. What could he do if the record-keeper claimed that there was no "interference with the privacy of a natural person" because all 10 principles were strictly observed - at present. There would then be no interference with privacy in terms of Clause 7, but since this is not an exclusive definition this would not prevent the Commission from investigating and making recommendations.

---

[84] Privacy Act of 1974, United States Code Title 5, s552a sub-s (b)(3); sub-s (8)(4)(D) requires all such "routine uses" to be published annually; see also Rule, p.102.

[85] ALRC22 [1321]

[86] ALRC22 [1323]

However, the absence of any wider "political basis of privacy protection" in the Principles, or any clear development of such a basis in the Report which could be used as an aid to interpretation,[87] would disadvantage the Commissioner in any such argument.

The Human Rights Commission, although not so directly tied to the Principles in its function of making general privacy recommendations,[88] might be similarly disadvantaged.[89]

The absence of these wider criteria in the Principles could therefore assist in legitimating systems which may in fact pose long term threats to privacy.

In our view, the Principles would benefit from the inclusion of some additional principle recognising these "external", political criteria for privacy protection.

3.6 "SOCIAL JUSTIFICATION": A MISSING PRINCIPLE?

It is difficult to formulate an adequate mechanism to implement the wider criteria we have discussed. The only attempt at some such formulation, of which we are aware, was what could be called the "social justification principle" in the NSWPC Guidelines,[90] which provided that "a personal data system should exist only if it has a general purpose and specific uses which are socially acceptable." This proposed principle was noted by the Commission but not discussed.[91]

The NSWPC principle is too vague, but we suggest that this "social justification principle" should be reworded and inserted as an additional principle in the Information Privacy Principles. A possible wording is "A person should not establish or continue a practice in relation to personal information the purpose for which is contrary to law, human rights, public policy or Government policy".

In summary,[92] the reasons why such an additional Principle is needed are:

(i) because the "purpose" of a system can be defined so broadly as to place no limit on excessive collection and centralization;

(ii) because "relevance" and other limitations, if assessed "having regard to the purpose of collection", do not limit the collection, use or retention of information if it can be shown to be statistically "relevant";

(iii) because all debate must otherwise proceed on an assumption of continued use of the information for its intended (benign) purposes, and cannot take into account the danger of future misuse;

(iv) because such a principle is needed as part of the Information Privacy Principles, not as unrelated principles concerning discrimination or political liberty, if the reasons for an "Openness Principle" in privacy protection are to be properly understood.[93]

There are also other ways in which the Commission's proposals could be amended to take more account of this wider "political" dimension. The Privacy Commissioner's functions[94] could be extended by empowering the Commis-

---

[87] Clause 3

[88] Clause 10 (1) "... the function of making recommendations and suggestions in relation to the privacy of natural persons ..."

[89] Clause 10(2); see, however, S.9(1) and Article 17, Schedule 1 (the ICCPR), Human Rights Commission Act 1981 (C'th).

[90] NSWPC Guidelines, n 53, 3.1 above, "Part A. The Justification for the System, Guideline (1) Social Acceptability of the System's Purpose and Uses."

[91] See ALRC22 [638] and ALRC Discussion Paper No. 14 Privacy and Personal Information AGPS 1980, para 31.

[92] See 9.4 above and 4.1 below for details.

[93] See 4.1 below

[94] Clause 12

sioner "to inquire into any practice in relation to personal information the purpose for which is or may be contrary to law, human rights, public policy or Government policy". The Human Rights Commission's functions[95] could be extended in a similar manner. This may be appropriate given the Commission's responsibilities concerning a broader range of human rights issues than privacy. A reference to the Australian Law Reform Commission concerning this and other aspects of "the social implications of informatics" is a further possibility.[96]

4. "OPENNESS": ANOTHER MISSING PRINCIPLE?
4.1 THE NEED FOR OPENNESS

One of the Principles adopted by the OECD[97] is the Openness Principle:

> "12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."

The OECD explained that "The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle [equivalent to rights of subject access and correction]; for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data."[98] In other words, if a person doesn't know that an information system exists, or how information in a system is used or disclosed, then a means of obtaining such details is essential for any meaningful privacy protection.

We would go further and argue that the Openness Principle is the most important privacy protection insofar as the "external" or "political" criteria[99] are concerned. Protection against the unrestricted growth or repressive potential of information systems is likely to depend almost entirely upon means of public awareness of the existence, uses and interlinking of information systems, as such awareness is a prerequisite for the development of the necessary political response.

In referring to this principle the Commission notes comparable provisions in Swedish, U.S., West German, Israeli and Canadian statutes[100] and the corresponding Public Access Principle in the Guidelines of the N.S.W. Privacy Committee.[101] There is no further discussion of the Openness Principle, nor any mention of the related term "public participation".

Given the Commission's statement that it formulated its general principles "drawing primarily on the OECD's guidelines",[102] it is surprising that no such requirement appears in its Principles. There is no explicit rejection of the Openness Principle as a necessary privacy protection; indeed the Commission makes a number of related recommendations. The implication of these recom-

---

[95] Clause 10
[96] ALRC22 [1413]
[97] Organisation for Economic Co-Operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris, 1980 (hereinafter OECD Guidelines)
[98] OECD Guidelines, p.31
[99] As discussed in section 3 above.
[100] ALRC22 [603]
[101] ALRC22 [638]
[102] ALRC22 [1195]; NSWPC Guidelines n XXX, 3.1 above, Guideline (6) Public Access

mendations is that an adequate implementation of the Openness Principle for privacy protection will be provided by the existing freedom of information legislation,[103] supplemented by a number of measures in the Draft Bill and the Principles[104] and the Human Rights Commission's "collation" role.[105] Each of these means of implementation will now be examined.

4.2 THE HUMAN RIGHTS COMMISSION'S "COLLATION" ROLE

This function of the Human Rights Commission (HRC) is explained as follows:

> "So far as the Commonwealth public sector is concerned, efforts should be made to publicize the existence and nature of record-systems containing personal records. The matters recommended by the Ontario Report [publication of an 'Annual Systems Notice' for each information system[106]] should be regarded as the minimum to be published. To some extent, the publication requirements of the Freedom of Information Act 1982 will help to publicize the existence and operation of public-sector record systems that include personal information. The HRC, as part of its general research and public education functions, should collate this information so that it can be published together for ease of reference. The HRC should encourage major private-sector record-keepers ... to include similar details in the compendium."[107]

The "publication requirement" of the Freedom of Information Act[108] requires, inter alia, "a statement of the categories of documents" maintained by a record-keeper.[109] The Ontario Annual Systems Notice requires considerably more, including:

> "4. the principal uses of the information and the categories of users to whom disclosures from the system are typically made; ...
> 6. the policies and practices applicable to the system with respect to storage, retrievability, access controls, retention and disposal of information ..."[110]

The above description of the HRC's role seems ambiguous. Is it to collate only the existing statements of categories of documents "for ease of reference", or is it to "collate" far more than that? It is also unclear whether the Commission evaluated the significant extra cost of such additional requirements, or compared their effectiveness with other alternatives.[111]

4.3 ANCILLARY PROPOSALS

Indirect recognition of the inadequacies of freedom of information legislation for privacy protection is provided by several of the Commission's less central proposals.

---

[103] ALRC [1208]; see section 4.4 below; for further discussion by the Commission of freedom of information see [15-16, 67, 632-34, 827, 984-1004, 1197, 1207-08, 1238, 1241, 1244, 1251-74, 1278-90, 1341-72, 1408]
[104] See 4.3 below
[105] ALRC22 [1208]; see 4.2 below.
[106] ALRC22 [1207]
[107] ALRC [1208]
[108] Freedom of Information Act 1982 (Cth), hereinafter "FOIA"
[109] S.8(1)(a)(iii)
[110] Ontario Commission on Freedom of Information and Individual Privacy, Public Government for Private People, Vol. 3 Protection of Privacy (1980), p. 683; cited in ALRC22 [1207]
[111] ALRC22 [1328-1337]

Principle 2 provides that "a person who collects personal information should take reasonable steps to ensure that ... [the record-subject] is told ... of his usual practices with respect to disclosure of personal information of the kind collected". Although this represents an apparently significant privacy protection, the words "is told", if read literally, place an obligation on the collector to cause communication to take place even when none is really needed. An example of this would be the collection of data from a customer on every occasion that a credit purchase in a retail store is made. The requirement is derived, at least in part, by a misunderstanding of the OECD guidelines. The Report states that "[OECD] Principle 9 requires that [the record-subject] be told the purpose for which [the information] is being collected".[112] The active word in OECD Principle 9 is "specified", rather than "told", and the Explanatory Memorandum is quite explicit that "such specification ... can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies."[113]

Principle 2 is subject to another significant weakness: it is qualified by the words "... before he collects it or, if that is not practicable, as soon as practicable after he collects it ...". The record-subject's ability to find out the purpose is therefore limited under Principle 2 to the time of collection. In practice only a small minority of record-subjects will have any interest in being told the purpose at that time. Only a small minority are ever likely to be interested at all, and these only at the time that the matter is actually of concern to them. The interests of the record-subject are best served by being able to find out , at any time, the purpose for which data is retained. The interests of the data collector and the record-keeper are best served by supplying information only when the record-subject actually requests it. Principle 2, if implemented in its present form, would have the effect of requiring a vast amount of data flow that is quite unnecessary, with all the attendant costs. It would please no-one.

Other surrogates for the missing Openness Principle are found in the Draft Bill. A record-keeper is to "take reasonable steps to help the person to make a request that complies with [the requirement to] provide such information as is reasonably necessary to enable the record to be identified".[114] He is further to "take reasonable steps to help the person make the request to the appropriate record-keeper".[115] He is also to give a person "a reasonable opportunity to make a submission to him about the matter" prior to refusing access on the grounds of insufficiently precise identification of the record or "substantial and unreasonable interference with [the record-keeper's] ordinary work".[116] These provisions enable a person to explicitly or implicitly find out about a record-keeper's "practices or policies", although only in the context of a request for access to or correction of a record of personal information.

4.4 FREEDOM OF INFORMATION ACT (FOIA) DEFICIENCIES.

The FOIA provides for publication of agency statements[117], the availability to the public of manuals and similar documents,[118] and a right of access to agency documents subject to a variety of exemptions and qualifications.[119] Of

---

[112] ALRC22 [1210]
[113] OECD Guidelines op.cit, para 54
[114] Clauses 70(1) and 51(3), corresponding to FOIA s.15(3)
[115] Clause 70(2); cf. FOIA s.15(4)
[116] Clauses 77, 51(3) and 76(1); cf FOIA s. 24(3)
[117] S.8
[118] S.9
[119] Parts III and IV

some 450 Commonwealth agencies, there are currently 24 which are exempt in full, 19 which are "exempt in respect of particular documents"[120] and fifteen classes of exempt documents[121] which may be invoked by any agency.

There are a number of reasons why the FOIA is of limited benefit as a means of privacy protection:

(i) The exemptions to freedom of information are not qualified by the existence of an intermediary, in the sense of an independent body or person who can exercise access rights on behalf of the public. This contrasts to the intermediary role of the Privacy Commissioner under the Draft Bill in respect of records of personal information.[122] The FOIA may need to be used by a record-subject to obtain access to any information necessary for rights of correction under the Draft Bill to be complete and effective. This may be so where access to "implicit information", stored rules or programs is necessary.[123] Where this occurs concerning a record which is exempt from the FOIA, the lack of intermediary access may mean that corrections which should be made cannot be made. The right of correction under the Draft Bill, in these instances, is made subject to the existence of a right of access under the FOIA. This result is no more justifiable than the nexus between access and correction under the Draft Bill.[124]

(ii) The most important limitation is simply that freedom of information legislation does not apply to the private sector at all.[125] The Commission's general approach is that information privacy principles are applicable to both the public and private sectors,[126] but in this context the only conclusion and recommendation seems to be that the HRC should collate and publish private sector information.[127] This falls far short of an openness principle, or even freedom of information, in the private sector.[128]

---

[120] S.7 and Schedule 2

[121] Ss33-47; Exemptions are provided, under certain circumstances, for Executive Council and Cabinet records, defence, security and inter-governmental records, records relating to the national economy, records relating to law enforcement and public safety, contempt of Parliament or courts, certain companies or securities records, records that are internal working documents, financial or property records, records concerning examinations, management and industrial relations, records subject to legal professional privilege, trade secrets and commercially valuable records, confidential records, and records relating to other persons or to incompetent persons.

[122] See 5.3 below

[123] See 6.3 below

[124] See 5.2 below

[125] There is a minor exception that documents originating in the private sector and in the possession or under the control of an agency or Minister may be accessible.

[126] See ALRC22 [1048, 1051, 1239, 1254]

[127] ALRC22 [1208] (Section 7.2 above)

[128] The claim in ALRC22 [1409] that "The Commission's proposals adopt and, so far as relevant, ... apply to private sector record-keepers ..., the basic entitlements and exemptions under the Freedom of Information Act 1982" [1409] must refer only to the subject access and correction provisions, as it cannot refer to access to information about "developments practice or policies".

4.5 CONCLUSIONS

A final concern relates to the Commission's suggestion that a national approach to information privacy should be negotiated between the Commonwealth and the States.[129] Yet the Commission's proposals have been shown in this section to be incomplete in their own right, in that they assume a previous or parallel implementation of freedom of information legislation equivalent to the Commonwealth FOIA. The Commission notes differences that already exist in the Victorian Act.[130] No other State has legislated for freedom of information. Therefore, if the principles are to be applied to the States, inclusion of an Openness Principle is necessary.

The OECD pointed out that the Openness Principle was essential for effective subject access, and so even from an "internal" perspective the Commission's approach may be criticised. We have argued openness is also essential when broader, "external" criteria are considered. We doubt that the Commission considered openness to be of such importance; it has certainly given it a more limited role. However, the Report does not seem to contain the Commission's full argument for even that limited role. Too much of the argument is left to inference from the existence of freedom of information legislation, and the ancillary provisions in the Principles and the Draft Bill.

5. ENFORCEMENT OF RIGHTS OF ACCESS AND ALTERATION: EXEMPT RECORDS AND INTERMEDIARY ACCESS.

5.1 ACCESSIBLE AND EXEMPT RECORDS

The Draft Bill proposes two main classes of records, those which are open to access by the record-subject under Clause 52, and those which are exempt from such access under Clauses 53-56. The extensive exemptions are based on those under the Freedom of Information Act 1982. It is beyond the scope of this paper to examine them in detail.[131] We will refer to records as "accessible" or "exempt".

The purpose of the exemptions is, however, "to ensure that the privacy interest protected by a right of access is properly balanced against other legitimate interests", including "the interest of society at large", "the interests of record keepers", "the interests of third parties and, it is said, of the record subjects themselves".[132] The choice of these particular exemptions is explained as follows:

> "The Commission does not propose to examine the issue of which classes of information should be the subject of exemption from rights of access

---

[129] "A national approach to protection of privacy will be needed, at the very least, in relation to information practices ... The standards recommended in this report could form the basis of a national scheme ... The Commonwealth should ... institute negotiations ... between itself, the States and the Northern Territory, to achieve agreement on the setting and enforcement of privacy standards throughout Australia": ALRC22 [1092]

[130] ALRC22 [632-34]

[131] See n.121, 4.4 above

[132] ALRC22 [1250]

under privacy legislation. Closely related questions have been the subject of lengthy debate when the Freedom of Information Act 1982 was before the Parliament. The regime governing access to records of personal information should be the same, so far as is possible, as the Freedom of Information Act 1982. It would be undesirable to have two different regimes for access to records held by Commonwealth agencies."[133]

"The decision ... [in 1982] was taken on the basis of the character of the information contained in the record, not the identity of the record-keeper. It is appropriate that [the exemptions] also apply in relation to access to personal records in the private sector"[134]

The Commission admits a qualification to the applicability of these exemptions: "The general interest of the individual as a citizen or resident of Australia, in having access to public sector documents is not the same as the interest of the individual in having access to records of personal information about himself".[135] This qualification is not explored in any detail in the Report.

Access to an "edited" exempt record may be available: "Before refusing access to an exempt record, the record-keeper must consider whether the matter in the record that makes it an exempt record can be edited out, without making the remaining parts of the record misleading".[136]

5.2 ALTERATION OF EXEMPT RECORDS

An exempt record may be just as inaccurate, misleading, out-of-date, incomplete or irrelevant as an open record. The record-subject's interest in having alterations to such records made under Clause 68 is no less because they are exempt from access. In some classes of exempt records, notably law enforcement and security records, the record-subject's interest in accuracy, completeness etc. may be of compelling importance. Nor is there likely to be any interest of the record-keeper or "society at large" in maintaining inaccurate, out-of-date records. In short, the justifications for exempting certain records from subject access do not justify exempting them from subject alteration.

The Commission's intentions on this matter are unclear. "The right to amendment ... should not be limited or restricted", it says.[137] It criticised the right to compel amendment under Part V of the Freedom of Information Act 1982 as too limited:

"... the right to amendment is limited to documents to which access has been obtained under [that Act]. The right to compel amendment is not available if access ... has been given gratuitously - outside the Act. If there is no right to compel access, there is no right to compel corrections."[138]

Consequently, the Commission recommends that "Whenever a person obtains access to records ... about himself, whether as required by law or gratuitously, he should be able to compel ... correction ..."[139] This still makes the right to compel amendment dependent upon the obtaining of access (by law or gratuitously). We cannot see why such a nexus is necessary.

How has the Commission implemented this approach in the Draft Bill? Our conclusion is that, in practice, a person might not be able "compel"

---

[133] ALRC22 [1253]
[134] ALRC22 [1254]
[135] ALRC22 [1255]
[136] Notes to Clause 75
[137] ALRC22 [1280]
[138] ALRC22 [1279]
[139] ALRC22 [1280]

correction of exempt records. We will examine whether alteration is possible under Clause 68, or otherwise.

Does Clause 68 allow alteration of exempt records? The exemptions in Clauses 53-66 are not expressed to apply to Clause 68, and only refer to "access". However, Clause 68(3) requires a request for alteration to "give particulars of the matters in respect of which the record is considered to be inaccurate, out-of-date, misleading, incomplete or irrelevant". How is a person who is denied access to the record because it is an exempt record able to give such particulars so as to make a valid Clause 68 request? The Privacy Commissioner's power to direct a record-keeper to make alterations to a record under Clause 92(1) can only be exercised "on the application of a person who has made a request to a record-keeper under section 68", which seem to require a request in conformity with Clause 68(3). Clause 70, concerning a record-keeper's obligations to "take reasonable steps to help the person make a request", only applied to requests for access, not alteration.

One possibility is that the record-subject might "guess" what items on their unseen record (if it exists) might require alteration, and request some possibly appropriate alterations. There is, after all, no requirement in Clause 68(3) that the particulars be accurate, and Clause 92 allows the Privacy Commissioner to direct alterations other than those particularized in the request. Such imaginative, or perhaps fictional, compliance with Clause 68(3) might be effective, but it seems unlikely to have been intended by the Commission. Clause 68 seems to contain a genuine "Catch 22".

Does the Draft Bill allow any alternative avenues to achieve alterations of exempt records? Clause 12 is wide enough to allow the Privacy Commissioner to inquire into a complaint that an exempt record may contain matters which should be altered. Clause 12 contains no requirement that the matters requiring alteration be particularized, only that the complaint be about a "specified act or practice". Clause 18 allows the Commissioner to require the record-keeper to produce a copy of the record concerned, and no exception is provided for exempt records. Clause 18(2) contains much narrower exemptions.[140] The Commissioner may then make recommendations that alterations be made to the record under Clause 21(2). Clause 21(4) may then have the anomalous result that the Commissioner is required to "give to the complainant a statement in writing setting out the results of his inquiry ... including particulars of any recommendations", which may of course result in the indirect disclosure of the existence of contents of an exempt record.

The result therefore seems to be that, in practice, the Commissioner would only be able to give directions for alterations to accessible records, and in the case of exempt records would only be able to make recommendations. In our view this distinction unnecessarily limits the right to obtain alterations. The Draft Bill could be amended to overcome this by provision that Clause 92(2) directions may follow from either Clause 68 requests or Clause 12 complaints, or by amendment to Clause 68. Clause 21(4) may also need to be made subject to a proviso similar to Clause 92(6).

---

[140] In summary, prejudice to security, defence, or international relations; disclosure of inter-governmental communications which would prejudice inter-governmental relations; disclosure of Executive Council or Cabinet deliberations; and other reasons which would support Crown privilege, but only if the Chairman of the HRC agrees.

5.3 INTERMEDIARY ACCESS AND CORRECTION

The Commission uses the expression "intermediary access" in a very limited way, to cover only those situations where a record-keeper reasonably believes that to give a person "direct" access to their record may cause the person harm.[141] Clause 85 provides that in such situations the record-keeper may require the person to nominate an "appropriate" intermediary, to whom access to the record will then be given. What right or obligation the intermediary then has to disclose the record to the person is left unresolved by the Report and the Draft Bill.

There is a more important sense in which the Draft Bill provides an "intermediary" form of access and correction rights. As argued above, in respect of exempt records, an "intermediary" is exactly how the role of the Privacy Commissioner is best characterized. Once this is recognised, it is apparent that the principles of subject access and alteration are left far more intact by the Draft Bill than might at first appear to be the case. Seen in this light, rights of access and alteration remain applicable to almost[142] all personal records, as the function of the exemptions is only to designate those situations where intermediary access, rather than direct access, is appropriate.

The Commission does not explicitly recognize the Privacy Commissioner's role as an intermediary, although there is some implicit recognition in the case of police information.[143]

If this reasoning is accepted, then it becomes questionable whether the Privacy Commissioner needs to be the intermediary in all cases. In some cases the record-subject may be able to nominate a perfectly "appropriate" intermediary to exercise access rights and make requests for correction on their behalf.[144] In some cases the record-subject may trust such an intermediary more than the Privacy Commissioner, who they may perceive as just another government official. In other situations the record-keeper may prefer to nominate an "appropriate" intermediary other than the Privacy Commissioner. This may be so in some national security or criminal intelligence matters.

Intermediary access could be classified in terms of record-subject nominees, record-keeper nominees, intermediaries by consent (where both must agree), and appointees (for example, the Privacy Commissioner). Which type of intermediary would be appropriate would depend on the particular exemption.

6. RIGHTS OF ACCESS AND DATABASE TECHNOLOGY

Today's "state of the art" in information technology is tomorrow's antique. It is clearly important that any information privacy proposals enacted now should be as independent of current conceptions of technology as is possible, if early circumvention by technological change is to be avoided. It is therefore informative to consider some relatively recent developments in

---

[141] ALRC22 [1242]

[142] The only records to which no form of access and correction, whether direct or by intermediary, are applicable, are records falling within the exemptions to Clause 18(2).

[143] ALRC22 [1418]

[144] In the Coombe-Ivanov Royal Commission into national security matters, Counsel acting for various parties have acted as intermediaries in a similar fashion.

database technology to access whether the Commission's proposals could give people effective access to information about them held in such databases.[145]

6.1 CONVENTIONAL DATABASES

In most conventional information systems, every record which contains information about a certain person contains some information which uniquely identifies that person, such as their name or an identification number. Whether or not the record is primarily about that person or someone else, the system operator will have indices of some type enabling access to the record via a unique identifier for that person. The effect of rights of subject access in such databases is simply to allow access to all records accessible via a unique identifier, and presents little problem in most cases.[146]

6.2 RELATIONAL DATABASES

With more recent relational databases it is possible to retrieve information about a particular person not only from records which contain an identifier to that person (and are therefore explicitly "about" them) but also from records which contain no identifiers to that person. This is made possible by the use of "rules of the system" which posit relations between the data items held in different records. A simple example is a database which stored details of a person's spouse, children and parents on that person's record, but by a "stored rule" allowed deductions to be drawn as to who a person's parents-in-law were, even though that information was not explicitly stored in the person's record or in any record identifying them. Such information about the person can be said to be "stored implicitly" in the database.[147] In order for a person to obtain access to all the information "about" them, in the sense of information which may be used to make decisions affecting them, they would need to have access not only to explicit information but also to implicit information. Unless the system operator discloses all possible implicit information which the stored rules could be used to generate, it would seem necessary to disclose the stored rules to the person and then to let them have access to such further implicit information (if any) as they decided they needed.

As an example of the potential privacy dangers of the use of relationship databases, consider the Costigan Commission enquiries.[148] The Costigan Commission developed "a structured database" from "public and government records, the records of financial institutions and the personal records of the people being investigated and the people with whom they dealt".[149] The system's "personal indexing system" captures against a person's name virtually any information known about the person's characteristics, history, associates or actions.

---

[145] For a full discussion see: Thom, J.A. and Thorne, P.G. "Privacy Legislation and the Right of Access", Aust. Comp. J., Vol. 15 No. 4 (1983) pp. 145-50; Greenleaf G.W. and Clarke, R.A. "Database Retrieval Technology and Subject Access Principles", Aust. Comp. J., Vol 16 No. 1 (1984) pp 27-32; and Thom, J.A., and Thorne P.G. "Privacy Principles: Tacit Assumptions Under Threat" (elsewhere in this issue).

[146] There may be, however, some conventional databases where information about a certain person is contained in a record which does not contain any unique identifier for that person, but can be accessed if some item of information external to the record, such as the record's disk location, is known.

[147] We use "relational" to include deductive databases; see Greenleaf and Clarke, n.142 above.

[148] The Royal Commission on the Activities of the Federated Ship Painters and Dockers Union.

[149] Meagher, D. "Computer Use by the Costigan Commission" Law and Technology Seminar Papers, Vol.II, Brisbane, 1983.

"By use of link analysis, the system can be employed to produce all known associations of a specified individual, whether the association is direct or indirect. Indeed, if all links between two specified persons are needed to be known, the system can produce all the paths between the two, even if there are several intervening persons".[150]

Criminal intelligence raises special problems for the operation of any information privacy principles, which are beyond the scope of this paper, and we merely raise the matter as an illustrative relational database.[151]

6.3 FREE-TEXT DATABASES

Free-text retrieval technology, which involves databases containing the full text of documents (newspaper articles, letters, telephone transcripts, court judgments etc.), raises somewhat different problems. Unstructured, discursive information has until now resisted widespread inclusion in computerised databases. Free-text systems have the potential, at least when coupled with technology such as optical character recognition (OCR), of enabling the creation of computerised databases containing vast amounts of personal information culled from a multitude of sources, but without the need for expensive structuring of the information during data capture.

In one sense, subject access is facilitated by free-text systems, because it is of the essence of free-text retrieval that every instance of a person's name or other identifier occurring in the database can be retrieved and displayed in the context in which it occurs. However, what is retrieved may be so discursive and extensive as to be virtually meaningless unless the person has some way of knowing which of it the record-keeper (or other users) regards as relevant to the making of decisions about that person. The user of a free-text system defines "relevance" partly by devising search commands which retrieve instances of that person's name or identifier only when it occurs in some specified conjunction with some specified words or phrases.

In practice, commonly used search commands are likely to be stored in a library of procedures, analogous to the "stored rules" of relational databases. However, this is not necessarily so. A search command may be used only once and discarded. How is the record-subject who obtains access to such a database to have any hope of anticipating or duplicating such a unique search? Even skilled investigators would have difficulty in knowing how to determine what the information "about" a person was in such a database.[152]

6.4 DATA AND INFORMATION

With relational and free-text databases, the underlying problem may well be the difference between access to data and access to information, by which we mean that "access to data" merely gives you the data in whatever form it happens to be stored, whereas "access to information" also requires the record-keeper to make the data meaningful by explaining the procedures by which the data is made relevant to decisions about individuals.

The difference between data and information can be illustrated by a hypothetical credit bureau or insurance bureau which maintained a computerised database of details of applicants' personal, employment, credit or insurance

---

[150] Ibid

[151] For discussion of the problems involve, see ALRC22[533], [1418] and Meagher, D. Paper IV "Gathering Information" and Paper V "Management of Information", Organized Crime (Papers presented to the 53rd ANZAAS Congress, Perth, 1983) pp 87-93, 138-40.

[152] See Greenleaf and Clarke n 142, 6 above.

history. However, contrary to normal practice in this country, it also maintained a separate computer program which "weighed" all these items according to a complex algorithm, and produced a "credit rating" or "insurance rating" which was not stored on that person's record at any stage, but simply produced in response to enquiries by users of the bureau and communicated to them. A person who obtained access to their "record" might obtain access to quite a lot of data, but possibly not obtain information as to why their recent credit or insurance applications had been unsuccessful, because they do not know what "weight" the various data items are given. They would also need access to the programs used to manipulate the data.

We may conclude that developments in database technology mean that for access rights to be meaningful they may also need to involve access to the "system rules" by which "raw data" is converted into meaningful information by the system's operators: stored rules, search techniques, and programs.

6.5 THE COMMISSION'S ACCESS PROPOSALS

The Commission proposes rights of access to "personal information":

> "Any information about a natural person should be regarded as personal information. Secondly, the link between the person and the information need not be explicit. If the information can be easily combined with other known information, so that the person's identity becomes apparent, the information should be regarded as personal information. Information should be regarded as 'personal information' if it is information about a natural person from which, or by use of which, the person can be identified."[153]

This is embodied in Clause 8(1) which provides in part:

> "Personal information means information or an opinion, whether true or not, and whether recorded in material form or not, about a natural person whose identity is apparent, or can readily be ascertained, from the information or opinion."

This definition excludes any other meaning of "personal information" unless a contrary intention appears. As we will subsequently discuss, the criteria of identifiability in Clause 8 may be significantly narrower than those recommended in the Commission's proposals.

A person's right of access under Clause 51(1) is not simply to "personal information" but to "a record of personal information about him". Clause 48 provides that "a reference ... to a record of personal information is a reference to ... a document that contains personal information ..." The definition of "document" in Clause 8(1) is of arguable scope,[154] but access is clearly access to a "record", not to "information" per se. Consistent with Clause 51, Principle 5 proposes access to "records of personal information".

Do these proposals or Principle envisage a right of access to implicit information or stored rules in a relational database? Would the Draft Bill allow such access? We suspect not. Consider the previous example of a relational database which contains a stored ruled about family relations which allows a person's record to be linked to that of their parents-in-law (even though the person is not identified in the parents-in-law's record). Would the Draft Bill allow the person access to their parents-in-law's record?[155]

---

[153] ALRC22 [1198]; See also ALRC22, p.1xii, Recommendation 56

[154] ALRC22 Vol. 2 p.268 says it "includes the widest possible range of methods by which information may be recorded or stored"; but cf Bayne, P. Freedom of Information, Law Book Co., Sydney, pp. 40-48 concerning similar provisions in S.3(1) of the FOIA.

[155] Leaving aside questions of "reverse FOI".

The principal question is whether the "natural person" in the Clause 8(1) definition of "personal information" must be the record subject, the "him" of Clause 51. If so, then it seems that the parent-in-law record will not "contain" (Clause 48) "personal information" (as defined in Clause 8) because the identity of the record subject is not "apparent" nor can it "readily be ascertained" from "the information" (that is, the parent-in-law record alone). It will therefore not be a "record of personal information" under Clause 51, and access to this "implicit information" will therefore not be available.

The contrary argument is that you can "readily ascertain" a person's identity from their parent-in-law's record by using the stored rule. This requires "natural person" in Clause 8(1) to refer to the parents-in-law. It also simply assumes and asserts that there is a right of access to stored rules, in order to argue for access to implicit information, and such a step is very doubtful.

A stored rule will not of itself be "a record of personal information", and Clause 51 will therefore not allow access. Clause 70(1) requires a record-keeper to take "reasonable steps" to help a person comply with the requirement of Clause 51(3) that requests for access "shall provide such information as is reasonably necessary to enable the record to be identified". On a very liberal interpretation, this could require disclosure of stored rules. Clause 83 provides that access "may be given in any appropriate form", but this does not seem to require disclosure of stored rules, even if it could facilitate voluntary disclosure.

An alternative is to attempt to use the provisions of the Freedom of Information Act 1982 to obtain details of stored rules,[156] but it does not seem sensible that information necessary for privacy protection should have to be obtained through another Act. A complaint to the Privacy Commissioner might succeed, but the right of access should stand on its own merits. It may at any rate be difficult for the record-subject to sustain an argument that a failure to disclose stored rules is "an interference with the privacy of a person", because Principle 5 is also subject to the definition of "personal information" in Clause 8(1).

If it is the Commission's intention that access to implicit information and stored rules be available, as we suggest is necessary for adequate privacy protection in the future, then the Draft Bill would benefit from clarification to put the matter beyond doubt.

The same arguments may apply to programs which must be used to make data held in a database meaningful. In the previous example of a "weighing" program,[157] the Commission's proposals seem to allow no access to the program. The Draft Bill could be amended to provide such access, or to require record-keepers to provide access to data in a form that is meaningful, a requirement that would go beyond the "appropriate form" of Clause 83.

7. ENFORCEMENT OF OTHER PRINCIPLES

7.1 SELECTIVE IMPLEMENTATION BY REGULATION

The ALRC sees the Principles as "statements of principle and aspiration"[158] to be implemented either voluntarily[159] or as a result of subsequent legislation.[160] Although the ALRC says "wherever practicable, mechanisms to give legal force to the principles should be provided",[161] the recommended

[156] There may be difficulties in obtaining information held in computer media under the FOIA: see Bayne in n 154 above pp.42-48.
[157] In 6.4 above
[158] ALRC22 [1200]
[159] ALRC22 [1054]
[160] ALRC22 [1415, 1418]
[161] ALRC22 [1201]

means of enforcement of Principles 1-4 & 7-10 are too limited.[162] The role of the Privacy Commissioner and the HRC in investigating complaints and making recommendations, using these Principles as a legislatively sanctioned "guide to proper information-processing practices",[163] is valuable but inadequate.

The exception to this limited approach to enforcement is Clause 115(1)(b), which allows regulations "prescribing the measures to be taken by persons specified in the regulations for the purpose of ensuring that records of personal information in the possession or under the control of those persons are securely stored and are not misused", and prescribing penalties for breaches. This follows the wording of Principle 4. We agree with the selective implementation of Principle 4 by regulations directed to those specific record systems where the need for adequate security standards is most acute. The very possibility of such regulations will make the voluntary implementation of Principle 4 more likely. It also avoid the necessity for subsequent legislation.

The scope of "misused" in Clause 115(1)(b) is unclear. Given that regulations are to be prescribed for "carrying out or giving effect to" the Act,[164] it could be argued that "misused" would encompass Principles 7-9 (Use) and 10 (Disclosure), all of which Principles deal with uses known to the record-keeper. Alternatively, it could be argued that "misused", used in the context of "securely stored", refers only to uses unknown to the record-keeper and caused by breaches of of security.[165] In either case "misuse" cannot extend to Principles 1-3 (Collection).

Why has the ALRC not recommended implementation by selective regulation of the remaining Principles 1-3 and 7-10? There is no explanation in the Report.[166] Clause 115 should be amended to enable regulations to be made to ensure that the records referred to are not merely "securely stored and not misused" but rather "collected, stored, used and disclosed in accordance with the Information Privacy Principles".

There can be adequate safeguards against misuse of this power. First, it is not within the Privacy Commissioner's or HRC's powers to promulgate regulations, only the Government's. Secondly, it could be provided that the Government receive the advice of the HRC before introducing regulations. Thirdly, the normal Parliamentary scrutiny of delegated legislation would apply. Fourthly, a record-keeper should be given, (and might already have) a reasonable basis to challenge the validity of any regulation which goes beyond reasonable implementation of the Principles. In this regard it is instructive that Principle 4 refers to "such steps as are, in the circumstances, reasonable", whereas Clause 115(1)(b) does not. The other Principles also have numerous references to standards of reasonableness. Such an approach would inevitably see the Federal Court and the High Court playing an important role in the interpretation of the Principles, and should ensure that they have a continuing development through amendment. It would make information privacy a dynamic rather than a static area of the law.

7.2 REMEDIES: DAMAGES, PROSECUTION, INJUNCTIONS AND CLASS ACTIONS

The ALRC rejected a remedy in damages for any breach of the standards embodied in the Information Privacy Principles, because of their role as guides

---

[162] See generally 2 above

[163] ALRC22 [1200]

[164] Clause 115(1)(b)

[165] This limited interpretation is supported by ALRC22 [1224] which refers only to "unauthorised" uses in explaining Principle 4.

[166] See ALRC22 [1225-1229], [1300], [1307]

rather than binding authority.[167] This argument does not apply to breaches of the enforceable rights of access and correction, nor would it apply to breaches of any regulations made under Clause 115. In these cases, such breaches should give rise to a remedy in compensatory damages as well as to the commission of an offence (under the Act or Regulations); such offences should be open to private prosecution. Injunctions against continuing breaches should also be available.

All of these methods of private enforcement should be obtainable by class actions. This is appropriate because whole classes of record-subjects may consider their present or future interests threatened by non-compliance, but individuals may have suffered insufficient damage to justify commencing proceedings against large record-keeping organisations. Furthermore, it means that affected individuals and public interest groups are not forced to rely on the Privacy Commissioner, HRC or prosecuting authorities to protect their interests. This is of particular merit, given that the principal threats to privacy are often seen as enamating from the State itself.

7.3 INFORMATION PRIVACY POLICIES WITHIN ORGANIZATIONS

As the ALRC stresses, many improvements to information privacy protection can be achieved through the adoption of voluntary guidelines[168] promoted by the Privacy Commissioner. At least with public authorities, this would be facilitated by measures which prompted record-keepers to think more seriously about their systems, such as

(i) the appointment of "Information Privacy Officers" (who could also be freedom of information officers in many cases) with the responsibility to report to the Privacy Commissioner on the extent to which their authority's personal record systems comply with the Information Privacy Principles; or

(ii) a requirement that "Privacy Impact Statements" be prepared and made publicly available before a public authority made substantial changes to a personal record system.

7.4 NOTIFICATION OF ADVERSE DECISIONS, AND LOGGING

The ALRC rejected as "unnecessarily costly" "a general requirement, whenever an adverse decision was made, to notify the person affected and to inform his of his rights".[169] In some record systems, however, such notification is essential to privacy protection, particularly where the record-subject may be unaware that the record keeper is using certain classes of information, or information from certain sources, in reaching an adverse decision. It is accepted as essential in credit reporting legislation.[170] It is accepted by public authorities in NSW which use criminal record information to make employment decisions.[171] Consequently, there should be provision for regulations to require such disclosure in such record systems and others where it is essential for privacy protection.

The same arguments apply to the necessity for logging all uses and disclosures in some record systems (notably credit reporting and criminal records). Indeed, the ALRC notes that logging could be required by regulations in selected systems, "as logging is an integral part of security measures.[172] There seems little justification for treating notification of adverse decisions any differently.

[167] ALRC22 [1082-1085], [1226-1227]
[168] ALRC22 [1054]
[169] ALRC22 [1397]
[170] See generally Greenleaf, G.W. "Credit Reporting", Consumer Sales and Credit Law Reporting Service, 1978-, C.C.H. Australia Ltd., Sydney.
[171] See generally New South Wales Privacy Committee, The Use of Criminal Records in the Public Sector, BP 41, the Committee, 1977.
[172] ALRC22 [1042]

TABLE 1: ALRC INFORMATION PRIVACY PRINCIPLES

Collection of personal information

1. Personal information should not be collected by unlawful or unfair means, nor should it be collected unnecessarily.

2. A person who collects personal information should take reasonable steps to ensure that, before he collects it or, if that is not practicable, as soon as practicable after he collects it, the person to whom the information relates (the "record subject") is told:

(a) the purpose for which the information is being collected (the "purpose of collection"), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law - that the collection of the information is so authorised or required;

(c) in general terms, of his usual practices with respect to disclosure of personal information of the kind collected.

3. A person should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out of date, incomplete or excessively personal.

Storage of Personal Information

4. A person should take such steps as are, in the circumstances, reasonable to ensure that personal information in his possession or under his control is securely stored and is not misused.

Access to Records of Personal Information

5. Where a person has in his possession or under his control records of personal information, the record-subject should be entitled to have access to those records

Correction of Personal Information

6. A person who has in his possession or under his control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, misleading, out of date, incomplete or irrelevant.

Use of Personal Information

7. Personal information should not be used except for a purpose to which it is relevant.

8. Personal information should not be used for a purpose that is not the purpose of collection of a purpose incidental to or connected with that purpose unless:

(a) the record-subject has consented to the use;

(b) the person using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person; or

(c) the use is required by or under law.

9. A person who uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of personal information

10. A person should not disclose personal information about some other person to a third person unless:

(a) the record-subject has consented to the disclosure;

(b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person; or

(c) the disclosure is required by or under law.