Impact on Practitioners of the A.L.R.C.'s Information Privacy Proposals

R. A. Clarke*

The Australian Law Reform Commission has proposed legislation to regulate information systems in order to protect privacy. Those proposals are summarised and their impact on information professionals assessed.

Keywords: privacy, data protection, regulation, information systems, professionalism, subject access, personal data, collection, storage, disclosure.

CR Categories: J.1, K.4, K.5, K.6, K.7.

1. INTRODUCTION

In April 1976 the Commonwealth Government referred the question of privacy issues arising under Commonwealth and Territorial laws to its Law Reform Commission. That body finally completed its study at the end of 1983, and this paper deals with the 'information privacy' issue which dominates its Report (A.L.R.C., 1983).

Unlike the recommendations of many similar overseas Reports, the A.L.R.C. proposes regulation not only of the information systems of government, but also of those of the private sector. Although Australia has lagged behind most other advanced western countries, these proposals would have an impact on information professionals to an extent not previously experienced overseas.

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. Its findings and recommendations will be the basis for debate on privacy issues in Australia for many years to come, and may also have significant impact overseas.

The Report's importance is more immediate than this, however. It makes quite specific recommendations to the Government as to what shape the regulatory mechanism over information practices should take. In December 1983, the then Attorney-General, a former member of the Commission, committed his Government to serious consideration of the Report.

This paper first identifies major documents in the recent history of privacy regulation around the world. It then presents an overview of the proposals contained in the Report. Finally, interpretive comment is provided on aspects relevant to computing practitioners.

2. THE RECENT HISTORY OF PRIVACY REGULATION

The term 'privacy' was little used in common speech or the law until the turn of the century. Improved standards of living saw ever more people expressing concern about liberties and individuality. By the 1960's there was serious, if confused, discussion of a variety of issues.

The U.K. was early off the mark with private members' bills in 1969. This resulted in the Younger Report (1972), reviewed in Goldsworthy (1973). A further valuable contribution to understanding of privacy questions was made by the Lindop Report (1978). Two Government White Papers of 1975 and 1982, accompanied by pressure from the country's European partners and competitors, resulted in the Data Protection Act 1984, reviewed by Niblett (1984) and Sterling (1984).

Sweden passed its Data Act in 1973. During the period 1977-1981 most of the countries of Europe enacted laws of a similar nature. These are well-documented in Pagano (1983) and in the Commission's Report, particularly in Volume III, which, as a concession more to economics than to technology, is available only on microfiche.

In the U.S.A., Westin (1967), Westin and Baker (1973) and the HEW Report (1973) were influential. The federal public sector was regulated by the Privacy Act (United States, 1974) and a report on the operation of that Act may be found in Linowes (1977). Many of the states enacted legislation of some kind during the 1970's (Smith, 1981). Canada's framework (1972, 1977, 1979, 1982) is also of relevance.

Developments in Australia can be traced back to Cowen's Boyer Lecture series (1969). This was followed by the Morison Report (1973) to the Standing Committee of Commonwealth and State Attorneys-General, reviewed by Goldsworthy (1974). With typical federal-state coordination, only N.S.W. acted upon its recommendations, creating the N.S.W. Privacy Committee in 1975. That Committee published an Exposure Draft of Guidelines for the Operation of Personal Data Systems (N.S.W. Privacy Committee, 1977).

Action in other States has been restricted to the regulation of specific matters, particularly aspects of consumer credit. Several states suspended consideration of the matter during the period of the Law Reform Commission's study.

The various European and the U.S. approaches differ in many respects. Access to interstate and international databases via telecommunications networks has highlighted the problems of inconsistency between laws in different jurisdictions. As a result, there have been efforts to achieve some level of international standardisation in the regulation of privacy, and of so-called Trans-Border Data Flows (TBDF).

Notable documents include those of the Council of Europe (1981), and the Organisation for Economic Cooperation and Development (OECD, 1981). The Chairman

* Department of Commerce, Australian National University. Manuscript received July, 1984; revised January, 1985.

of the Expert Group which drafted the OECD Convention was Mr Justice Kirby, then Chairman of the Australian Law Reform Commission, and the document is claimed in the Report to have been particularly influential on the Australian proposals. In December 1984, the then Attorney-General announced that Australia proposes to formally adhere to the OECD Guidelines.

3. OUTLINE OF THE COMMISSION'S PROPOSALS

(a) Overview

The Commission's actual proposals extend over several hundred pages, referring back to nearly five hundred pages of background material and several hundred of Appendices. Even the Summary of Recommendations contains 89 paragraphs extending over 25 pages (A.L.R.C., 1983).

The first volume of the Report analyses the threats to privacy, and summarises existing law. The second contains the proposals, including Draft Bills accompanied by explanatory notes. The Bills are not easily accessible to the layman, due to ". . . the highly technical and often unreadable language of our legislation . . ." (Kirby, 1983, p.62). In addition, privacy regulation must be fitted gently into a large complex of existing law. In particular, the Commission proposes a high degree of compatibility with the Freedom of Information Act, 1981. This was itself a version of the U.S. Act subjected to a significant amount of Parliamentary negotiation and compromise.

The proposals are presented in simplified form in this paper. Such gains as are made in brevity and readability are necessarily sacrificed in elegance, precision, sophistication and subtlety. References to paragraph numbers in the Report are enclosed in [square brackets], while clauses in the Draft Privacy Bill are in (round brackets).

* **Information Privacy Principles**
  to express government policy
  to guide organisations and individuals
  to provide the basis for complaint investigation
  to provide the basis for more specific laws
* **Privacy Commissioner and H.R.C.**
  to enquire into complaints
  to research into issues
  to resolve subject access complaints
* **Subject Access Rights**
  to create a right of access to data
  to create a right to request change to data

Fig. 1: The Proposals

The proposals are built upon three key and inter-related elements, identified in Figure 1.

(b) Information Privacy Principles

The key element in the Commission's proposals is a set of ten Information Privacy Principles (Figure 2). These are intended as general principles applicable to virtually all information systems involving information about identifiable people. "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" [1200].

Because the principles are of such general application, they do not set out to provide the full extent of protection

Collection of Personal Information
[531-535, 788-797, 1209-1221]

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; and
   (c) in general terms, of his usual practices with respect to use 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
[543-579, 1011-1030, 1222-1224]

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
[979-1010, 1230-1277]

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
[979-1010, 1278-1291]

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
[119-133, 536-542, 798-978, 1292-1300]

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 or 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
[119-133, 536-542, 798-978, 1292-1293, 1301-1327]

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 using 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.

Fig 2: Information Privacy Principles

which may be necessary or desirable in some information systems. The Commission sees more detailed sets of principles being developed for specific classes of system, and implemented either voluntarily [1054] or as a result of subsequent legislation [1415, 1418]. In addition regulations can be made, in particular to ensure that records "are securely stored and are not misused" (Cl.115(1)(b)) and [1399, 1402].

The ten general Principles are to be given legislative approval as "the basis for the protection of privacy in the information processing context" [1200]. This is to be achieved by including them as Part II of the Schedule to the Draft Privacy Bill. The Commission notes that "this is a novel approach to implementing general principles in Australian law", but the U.K. Act (since enacted) is similar in this regard.

(c) Privacy Commissioner Within the H.R.C.

The Commission argues that a 'statutory guardian' is needed [1039-1066, 1228-1229]. It recommends that there be a Privacy Commissioner, and that he be a full-time member of the Human Rights Commission (Cl.11). Some of the functions of the statutory guardian would rest with the Human Rights Commission as a whole, including public education and the making of recommendations to Government and other bodies on privacy issues (Cl.10(1)).

Other functions, including those of inquiring into, and making recommendations concerning particular complaints (Cls.12,21), are to be exercised by the Privacy Commissioner. The Commissioner's function of dealing with complaints is dealt with in the following section.

(d) Subject Access Rights

The Commission proposes that two of the Principles are sufficiently clear and precise, and sufficiently central to the protection of privacy, that they should be implemented immediately. Those two principles are numbers 5 and 6 concerning subject access to records and correction of information.

A person's right of access to a record of personal information (Cl.51) is to be subject to a number of exemptions, most of which are based on the exemptions under the Freedom of Information Act 1982. They have been adopted because of what the Commission sees as a "need for harmony" with that Act [1253-55, 1281].

In addition, "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 appropriate alterations to the record (Cl.68). This replaces the more limited right found in Part V of the Freedom of Information Act 1982, which was only intended as an interim measure [1279].

4. THE COMPLAINTS MECHANISMS

Different control regimes are proposed for complaints about subject access and alteration, as distinct from other information privacy matters.

(a) General Privacy Complaints

Alike with overseas privacy legislation, 'privacy' is not defined in the Draft Bill [19, 594]. However, Clause 7 of the Draft Bill provides that:

> "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*" (my emphasis).

The Schedule contains the Information Privacy Principles, hence the failure of an organisation to comply with the Principles will be sufficient to give the Privacy Commissioner jurisdiction to inquire into a complaint of interference with privacy (Cls.12,21). The powers of the Human Rights Commission are expanded analogously (Cl,10(2)).

The Privacy Commissioner would have considerable investigative powers, including the ability to call compulsory conferences (Cl.16), to compel the production of evidence (Cl.18), and to hold an inquiry in whatever manner and considering whatever evidence he thinks fit (Cl.17). There are no formalities required of a complainant.

These powers are balanced by constraints (Cls.18-24), such as all parties having reasonable opportunity to provide information to the Commissioner prior to the matter being determined, and the findings being given to the complainant and the organisation responsible for the alleged interference.

The Commissioner's ability to enforce any finding he reaches is very limited. Apart from exercising powers of persuasion, his only other recourse is to convince the H.R.C. to recommend changes in law or practice; his position is that of a conciliator, not an arbitrator [1041, 1052-1070].

(b) Requests for Subject Access

Part V of the Draft Privacy Bill creates a far more powerful regime relating to 'records of personal information'. "A person who wishes to obtain access to a record of personal information about him may make a request to the record-keeper for access to it" and, in general ". . . the record-keeper shall give the person . . . access to that record" (Cls.51,52), [979-1010, 1230-1277].

This right is subject to many express and implied *qualifications*:

(a) the applicant must find the *record-keeper*;
(b) the request must be in writing and sufficiently *specific* to enable the record to be identified (Cls.51,69,77);
(c) the applicant may need to understand the record-keepers' *practices and policies*;
(d) there are many classes of *exempt records* (Cls.52(2), 53-67,72,75) and with a few classes there is even no need for the record's existence or non-existence to be admitted. These exemptions parallel those of the Freedom of Information legislation and relate mainly to the public sector;
(e) requests may be refused if they would require 'substantial or unreasonable *resources*' (Cls.76,77);
(f) *charges* may be levied (Cls.52,86,87);
(g) considerable *time* may elapse before the record-keeper must respond (Cl.80), and deferment of access is possible (Cl.79). An appeal against an adverse decision would of course result in further delays;
(h) the requirement to inform the applicant of an *adverse decision* (Cl.82), need not be complied with; after elapse of sufficient time the failure is merely deemed to be a refusal, creating the possibility of an appeal (Cl.80(3));
(i) arrangements for the *exercise* of access rights in the company of advisers, by a voluntary intermediary or by proxy are not explicit within the Act, will depend upon other law and upon subsequent

administrative and judicial decisions, and will as a result be complex and constraining (Cls.51,52,83(2),85), [1242-1249, 1275-1277];

(j) there are *no sanctions* against a record-keeper who fails to comply with his obligations (Cls.101-102);

(k) by virtue of Cl.80(3), a record-keeper can avoid informing the applicant of his *rights* to have the decision reviewed;

(l) by virtue of Cl.80(3), a review or appeal may have to be commenced without knowledge of the *reason* for the refusal.

The interpretation of the access right may also prove a fruitful source of revenue for the legal fraternity. The meaning and scope depend upon a forest of definitions which parallel the Freedom of Information Act, and include 'a record of personal information' (Cl.48), 'document' (Cl.8), 'personal information' (Cl.8), 'record-keeper' (Cl.49) and 'control of a record of personal information' (Cl.47).

One major definitional problem occurs with 'record-keeper' which is '. . . the person who has the possession or control of the record' (Cl.49(1)), where control includes being '. . . in a position to obtain access to a record . . .' (Cl.47). This seems rather different from the discussion at [1199], and is apparently intended to cater for records stored outside Australia (Note to Cl.49).

Some of the most privacy-sensitive records are the joint or shared responsibility of several organisations; many people in many separate and dispersed sections of those organisations may have access; and another organisation entirely may have possession (typically a bureau or a wholly- or partly-owned data-centre subsidiary); hence there will be considerable uncertainty as to who has what responsibilities in relation to which data.

(c) Requests for Alteration of Information

A person may request a record-keeper to change a record of personal information that is inaccurate, out-of-date, misleading, incomplete or irrelevant (Cl.68). The word 'amendment' is used in the Report at [1278-1280 and 1383] and in the headings within the Draft Bill; the word 'correction' is used in Principle 6 in the Schedule to the Draft Bill. Both terms, in their normal usage, imply error or omission on the part of the record-keeper. If a neutral term such as 'alteration' were used, unnecessary stimulation of adversary attitudes could be avoided.

Unlike requests for access, there would be no requirement that a record-keeper comply with the request, even if it is justified (cf. Cl. 52).

In principle this right is not dependent on the prior exercise of the right of access. However in practice it would usually be necessary to have first seen the contents of the record, hence this right is largely qualified by the limitations noted above in relation to requests for access.

(d) Appeals Procedures

All decisions by record-keepers are subject to appeal to the Privacy Commissioner, who may direct the record-keeper to comply with all or part of the request (Cl. 92). Rejections of requests to Commonwealth agencies may be subject to prior internal review (Cls. 90,91). A right of appeal by either party to the Administrative Appeals Tribunal (A.A.T.) is proposed (Cls. 92(7), 94-99). From there an appeal would normally be allowed to the Federal Court (Cl. 103). There is no sanction for failure to comply with a direction of the Privacy Commissioner, but there may be in the case of A.A.T. and Federal Court decisions.

5. SCOPE OF THE PROPOSALS

(a) Type of Organisation

The proposals apply to *both public and private sector organisations* [617,1051,1239]. Comparable legislation in the United States and Canada applies only to public sector bodies, and in the United Kingdom many private sector operations are exempted.

The Commission considered itself unable to make recommendations regarding some classes of records of personal information concerning Australian citizens or residents, due to the constitutional limitations of the Commonwealth, and the terms of the Commission's Reference [7-10, 1036-7, 1396].

The proposals do not apply to State public sector bodies. They apply to *Commonwealth public sector bodies and to all bodies in the Territories,* but for this purpose, the Northern Territory and Norfolk Island, as self-governing Territories, are treated as States [1037].

Subject to the constitutional limitations, the general proposals also relate to private sector organisations. Clause 10(2) would empower the Human Rights Commission to inquire into ". . . acts done and practices engaged in by any person, whether in a Territory or not, by means of or in the use of a postal, telegraphic, telephonic or other like service" and which may interfere with privacy. It would seem that *many activities of private sector organisations throughout Australia* would come within this provision, particularly with the increasing use of data transmission and point of sale data capture. The Commission gives the examples of 'direct marketing through telephones' and 'direct mail' (Notes to Cl.10).

The more specific and onerous *access and correction rights* apply to 'records of personal information' that are in the Australian Capital Territory or the Jervis Bay Territory (Cl.45); also to records elsewhere in Australia about residents of those Territories (Cl.46(1)); and to records not in Australia about persons who ordinarily reside in Australia, provided they are 'under the control' of an Australian record-keeper (Cl.46(2)). For many private sector record-keepers, whether operating in the Territories or not, at least some data subjects would have legal rights of access to and correction of their records.

(b) Type of Recording Medium

The proposals apply to *both automated and manual record-systems* [118,589,1193,1413,1415], rather than just computer-based systems. In France, Luxembourg and Austria, corresponding legislation only applies to automated information systems (whether computerised or not). In the United Kingdom, judging by the term 'automatically processed information' in the statute's long title, the legislators intended to exclude 'manual' records. Since the data is regulated if it is ". . . recorded in a form in which it *can* be processed by equipment operating automatically . . ." (Section 1(2), my emphasis), and optical character and voice recognition technologies are increasingly enabling the printed and spoken word to be processed, the scope of the U.K. legislation seems far broader than intended.

(c) Status of Data Subject

The Draft Bill applies to *persons who 'ordinarily reside' in Australia,* which would appear to exclude most foreigners (including all tourists and those other than 'ordinarily' resident here), and even some Australian expatriates (Cls.45,46). Some of these exceptions may result from constitutional limitations.

(d) Uniformity Within Australia

The Commission notes that it is ". . . 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" [1393; see also 1088-92]. In tabling the Commission's Report, the then Attorney-General noted its call for uniformity and said that he would bring the matter to the attention of the Territories and the States (Press Release 184/83, Commonwealth Attorney General, dated 14/12/83). The Report also notes various heads of power under which the Commonwealth could extend the proposals [1396].

The Report is also is under consideration by some States, notably N.S.W. and Western Australia, both of whom deferred action during the late 1970's pending completion of the Commission's study.

6. APPROACHES REJECTED OR DEFERRED

In order to properly appreciate the nature of the proposals, it is useful to note some alternative or supplementary approaches which the Commission considered but rejected:

(a) Licensing. Revocable registration of at least some classes of record systems is part of the framework in the United Kingdom, West Germany, France, Sweden, Norway, Denmark and Israel. The Commission was not convinced that problems in Australia were such as to justify the sweeping controls normally associated with licensing [1073,1202-1206];

(b) Public Listing. Public listing of personal record systems and their uses is required in the United States and Canada. Although the Commission saw "considerable value" in this idea, it did not propose anything beyond the present requirements of the Freedom of Information Act 1982, perhaps augmented by a compendium to be maintained by the HRC [1207-1208]. The expense of public listing under the U.S. Privacy Act is noted [1335]. Whether it is effective, and whether the risk it creates is any less than that which it purports to overcome, are not discussed;

(c) 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 privacy' " [1075], was rejected as "too vague and nebulous" [1081, see also 1225-1227]. The Commission adheres to its related 1979 recommendation "that a new statutory tort regarding publication of sensitive facts be established" (see [1085 footnote 129], and A.L.R.C., 1979);

(d) Compensation For Breach of Standards. The possibility of a more limited remedy in damages was also rejected due to the generality of the principles [1082-5,1401]. Since the rights of access and alteration are framed with a great degree of particularity in the Draft Bill, it is quite possible that some such remedy may later be considered. Many countries, including the U.K., include such provisions;

(e) Notification of Adverse Decisions. Consideration was given to "a general requirement, wherever an adverse decision was made, to notify the person affected and to inform him of his rights". This was rejected as unnecessarily costly, but felt to be "thoroughly desirable as a good administrative practice", and commended for ongoing study by the H.R.C. [1397]. It is already practised in a few sensitive areas such as credit granting and criminal record access for job-applications;

(f) 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 Report notes the possibility of logging being required in particular areas by use of the regulations power [1402];

(g) Legal Persons. The question as to whether privacy protections should extend to corporations was deferred [27-29,1404].

7. FAIR INFORMATION PRACTICES

Rule (1980) identifies the approaches taken in most countries as reflecting the 'efficiency criterion' whereby information practices are generally regarded as acceptable provided they deal fairly with accurate data. He refers to this as the family of 'official responses' of Governments.

The Commission's proposals belonging to Rule's family. The Report itself refers to the 'emerging pattern' of laws around the world. The Commission accepted a range of arguments put to it by business, the public service and information professionals. The list of Consultants to the Commission similarly shows a bias towards information users, rather than towards representatives of consumers or citizens. The Report seeks to balance privacy against other interests [52-54], and addresses economic and administrative implications of its proposals [76-79,1325-1385]. The Commissioner responsible for the Report appeared to submit fully to the technological imperative: he considered privacy to be an already outdated concept, and nominated assistance to people to adjust to the loss of privacy resulting from technological change as the real task (The Australian, 15 December 1983).

The Commission cannot be accused of intemperate response to vague, sensationalist public concerns. Indeed it may have paid too little attention to the broader, political aspects of privacy and civil liberties. The OECD Guidelines include an *Openness Principle* which seems to underpin the effectiveness of the subject access mechanism. Without explanation [relevant passages are at 602-603,1195,1253-55, 1281 and 1399], and seemingly inexplicably, the A.L.R.C.'s proposals contain no such principle.

The Commonwealth Freedom of Information Act (FOI), passed in 1982, underwent its tortuous legislative progress during much of the Commission's work. There is no doubt that the two policy issues are closely related, and the Report is strongly influenced by it. Nonetheless, concern could be felt about the extent to which the proposals may have been distorted by its influence. FOI requirements have been adapted to by the Commonwealth public service with a speed and lack of disruption that has surprised the public and the public sector alike (FOI, 1983). But those requirements include a wide range of exemptions and are complex and specialised. Above all, they have almost no impact on the private sector. They therefore fall far short of being an adequate surrogate for the O.E.C.D.'s Openness Principle.

One of the particular shortcomings of so-called freedom of Information laws (one which is not shared by the New Zealand Official Information Act) is their focus upon documents, records or other *physical manifestations of information.* The desire for compatibility has resulted in this weakness being transmitted to the privacy proposals. The effect is that many applicants who are seeking information, rather than mere documents, may be easily, even unintentionally, frustrated by a record-keeper who operates to the letter of the law.

One aspect of the problem is the question of subject access to the rules whereby data is selected and the decision criteria whereby data is interpreted and becomes information. Thom and Thorne (1983 and 1984) and Greenleaf and Clarke (1984) investigated the matter in the context of relational, deductive, free-text, distributed and public access databases. They concluded that the subject access mechanism formulated by the Commission, alike with those in many other countries, was unlikely to satisfy the needs of data subjects in databases supported by any more advanced DBMS than straightforward hierarchical and network software.

8. IMPACT ON ORGANISATIONS

All organisations whose information systems deal with identified personal data need to assess the extent to which their systems comply with the proposed requirements.

This would, of course, involve the data capture, validation, updating, storage, culling, display and printing and data-interchange functions. These have been for the most part the responsibility of computing professionals, although the advent of fourth generation languages and end-user development have recently thrown doubt on the exclusivity of that role.

The activities impinged upon by the new privacy rules do, however, extend much further. The rules also affect data collection practices; the codification of data; the organisation's use of data; and the basis upon which information about individuals is disseminated beyond the organisation's boundaries. In many organisations such matters will be user responsibilities, beyond the scope of the senior Information Systems executive.

9. IMPACT ON INFORMATION PRACTITIONERS GENERALLY

In the event that the Draft Privacy Bill is enacted, practitioners of computing will have a number of new responsibilities. As a matter of professionalism and morality, some of these responsibilities arise merely because the A.L.R.C. has identified problems requiring resolution.

As a *first response,* it is necessary for practitioners to:

- acquaint themselves with the proposals;
- bring the matter to the attention of user and I.S. management;
- ensure that other practitioners are informed;
- encourage users and their managers to understand the A.L.R.C. proposals and prepare to comply with them;
- be prepared to argue the matter with user management.

To adapt *existing systems* to the new regulated environment, the following are necessary:

- assess existing systems for compliance with requirements;
- build into enhancement packages those modifications necessary to achieve compliance;
- be prepared to argue the matter with information systems management.

To ensure that *future systems* will comply, additional steps are needed:

- consider the Information Privacy Principles during the analysis and design phases, perhaps as part of the control and audit factors, alternatively as the first of a new class of external responsibilities;
- integrate the Principles into the software development methodology.

Beyond this, professionals have *broader responsibilities,* both to their employers and to the public. A degree of confusion can be anticipated, particularly in establishing who has what responsibilities. The commonsense approach would be for the organisation(s) which respectively collect, process, store, use and disclose to be responsible for compliance with the relevant principles, but the Report appears to assign all responsibilities to the 'record-keeper' [580-582,1199]. There may be excessive or unduly costly requirements (such as literal interpretation of Principles, especially No. 2); the Commission developed an appreciation of information technology, as evidenced at [101-133,280-282,531-585,1390-1391 and 1406], but the profession and the industry will need to ensure that the Privacy Commissioner and his staff quickly achieve and maintain at least the same level of understanding.

The practitioner's activities must therefore extend to the following:

- provide feedback to the Attorney-General, and later the Privacy Commissioner, on matters of technical difficulty, uncertainty, ambiguity, undue expense, etc;
- take part in the political process of law development.

10. IMPACT ON PRIVATE SECTOR PRACTITIONERS

Many computing professionals have regarded themselves as bastions of the free enterprise system, and have accorded low priority to understanding and complying with legal obligations. In recent years, as the quality of products being delivered has improved, the air of gambling once associated with the acquisition of data processing equipment has begun to dissipate. With this has come a significant increase in the number of cases involving contract and sale of goods law coming before the courts.

Many private sector organisations, which have hitherto been somewhat cavalier in their handling of personal data, will have difficulty adjusting to the new environment. Fortunately there are a variety of mitigating factors. Many organisations hold very little information of any real sensitivity, particularly those whose clients are exclusively corporations, and so would not be particularly visible to the Privacy Commissioner or the public. In addition, many of the organisations which hold sensitive data have already instituted security precautions, because in some respects at least, their own interests coincide fairly closely with those of their data subjects; this applies particularly to financial institutions. There has also been an upsurge in trade union concern about privacy interests of their members, and many organisations have already recognised the legitimate desire of their employees for access to their personnel files.

There will nonetheless be many computing professionals who will need to convince their employers and clients of the need to take prompt, and in some cases burdensome action to ensure that their systems comply with the privacy principles.

11. IMPACT ON PUBLIC SECTOR PRACTITIONERS

The environment in government departments and instrumentalities is quite different from that in the private sector. Awareness of legal requirements is a fundamental factor in the operations of government, and public sector employees have had to adapt to a variety of recent changes such as ombudsmen, environmental impact assessment, administrative appeals avenues, anti-discrimination measures, and equal opportunity initiatives.

The Commonwealth Freedom of Information Act, which came into effect on 1 December 1982, was of course especially relevant. The intent was to reverse the old default assumption of non-disclosure, and much has been achieved in a very short time.

The Act relates to information of all kinds held by government, but in practice, ". . . most of the requests have been for documents relating to the personal affairs of the applicant. . ." (F.O.I., 1983, p.xiii). Unfortunately, ". . . the reporting system does not provide information on . . . the number of requests for personal information" (p.67). A total of 5699 requests were received in the first 7 months, by 130 agencies (there are some 400 agencies subject to the Act, 24 exempt and a further 15 exempt in respect of their competitive commercial activities). Five agencies received over 70% of the requests (p.69):

Agency	%
Social Security	20.7
Commission of Taxation	19.8
Veterans' Affairs	18.5
Immigration and Ethnic Affairs	8.2
Defence	5.3

There had been to that date only 33 requests for amendment of personal records (p.75), but this is in part because such requests may only be made in respect of records to which access has already been granted under the Freedom of Information Act; few such cases had been possible in the first seven months of the Act's operation.

The original estimates by agencies of annual numbers of requests had been ". . . tentative, and in many cases admittedly based on little more than guesswork" (Senate Standing Committee, 1979, pp.72-74, 471-475). They were, for the most part, very high; and were in very few cases vindicated by the experiences of the first seven months of the Act's operation. Inferences will be more reasonably drawn following the release of the Annual Report relating to the first full year of operation, due in early 1985. It would be natural to anticipate a steady increase in the volume of requests as the mechanism becomes better known to the public. In addition, the experience of the N.S.W. Privacy Committee (1980) has shown that the volume of complaints is highly sensitive to issue-related publicity.

The costs of the Commission's subject-access proposals are likely to be subsumed within the costs of Freedom of Information administration. The creation of the FOI machinery was estimated to have cost of the order of $3 million, with running costs for the first seven months of 200 man-years or $8 million (F.O.I., 1983, pp.114-124). Some 200 of the originally anticipated 685 additional positions had been filled (pp.143-144). If the running costs had been incurred entirely in the handling of requests, this would have suggested an average cost of about $1500 per request, with a range from $572 (say 3.5 man-days) at Veterans' Affairs to $3800 at the Australian Federal Police (23 man-days).

The discrepancy against mythical private industry norms of $20 for a one-page letter is to be accounted for partly by start-up costs relating to documentation of agency systems, significant learning difficulties and excess capacity. In addition, ". . . many agencies have found handling requests to be more complex and expensive than they had anticipated . . ." (p.114). The Department of Industry and Commerce, for example, most of whose requests could be expected to be complex, non-privacy matters, reported 7.3 man-years (or $300,000) costs in dealing with 68 requests, or $4400 each (p.122).

Of over 4000 requests that had been determined by 30th June 1983, 62% were granted in full, 25% in part, and 13% refused (p.70). Almost all of the sixteen exemption classes were invoked, frequently more than one per refusal. Most commonly invoked was the privacy of persons other than the data subject, followed by the secrecy provisions of other Acts; enforcement of law and the protection of public safety; internal working documents; and breach of confidence (p.93).

During the years of discussion leading up to the introduction of the Act, many government agencies had expressed serious concern both at possible deleterious effects on their modus operandi, and at the administrative burden and costs involved. A number of concerns continued to be expressed at the date of the first Annual Report, but these were much more precise and constructive (pp.137-147). The section on 'positive benefits' (pp.127-137) further demonstrated that the public sector had come to terms with FOI far more quickly than even the optimists had thought possible.

The strength of the A.L.R.C.'s desire to present the subject access proposals as mere modifications to the established and accepted FOI arrangements is therefore readily understandable. The subject access mechanism is in fact little different from that already in existence [1230-1277]. Changes include: attempts at clarification of definitions, of scope and of access by intermediaries; additional provision for incompetent persons and children [1243-1249]; minor modifications to FOI exemption classes; and a proposed 'Reverse-FOI' procedure, whereby a data subject would be consulted if a third party sought information about him [1268-1269].

The amendment provisions were a late addition to the FOI Act, and were proposed by the Senate Standing Committee (1979) with rather less confidence than their many other recommendations (pp. 264-265). Indeed the A.L.R.C. goes so far as to see them ". . . as a stop-gap measure until the Commission's recommendations are implemented" [1003, 1279]. Two changes are that amendment is not now meant to be dependent on prior access, and (partial) relaxation of the anomalous limitation to Australian citizens and long-stay visitors [1278-1280].

The subject access provisions are likely to cause but few additional problems for information practitioners in the public sector, because the adjustments necessary are small in comparison with the effort already undertaken to implement the Freedom of Information Act.

However the (at present unenforceable) privacy principles relating to collection, storage, use and disclosure represent a new challenge.

12. IMPACT ON MEMBERS OF A.C.S.

A member of the Australian Computer Society undertakes to abide by its Code of Ethics (A.C.S., 1979, Articles 4.4,4.9). Article 7.1 is particularly relevant to the privacy issue:

> "A member shall have proper regard for the health, privacy, safety and general welfare of the public in the performance of his professional duties. In case of conflict between the general welfare of the public and the performance of his professional duties the interest of the public shall be put first."

The implications of this Article are far from clear; in particular 'general welfare of the public' is used ambiguously,

and the term 'professional duties' is nowhere defined. If, as would be reasonable to assume, 'professional duties' encompasses all of the 'standards of professional conduct' laid out in Articles 6 to 10 of the Code, then *a professional member's duty to the public is to be placed above his duty to his employer.*

Until now the standards of conduct in relation to most matters, and particularly to privacy, have remained sufficiently nebulous that the prospects of a member's performance being judged at all, let alone found wanting, has been remote in the extreme.

In 1975 the Society published a 'Code of Good Practice in The Privacy, Security and Integrity of Data'. There is no reference in the Constitution to this document. It is, moreover, phrased in such a way that it is difficult to construe as having any binding force. The A.L.R.C.'s view is that ". . . the code is a significant statement of aspiration, but it has not been widely implemented . . ." [1007]. Nor is there any other apparent constitutional basis upon which an Investigation Committee could depend in assessing a charge of unprofessional conduct in relation to a privacy matter.

The professional disciplinary body could of course refer to authoritative standards originating outside the Society. There are, however, few of these either. In some states there is relevant legislation concerning the consumer credit industry; and 'Guidelines for the Operators of Personal Data Systems' and 'Employment Guidelines' were published by the N.S.W. Privacy Committee (1977 and 1980). (The former were left in Exposure Draft form pending the release of the A.L.R.C. Report).

One of the effects of the A.L.R.C. proposal would be to provide a set of principles from which the responsibilities of computing professionals in respect of privacy matters could be derived.

The possibility therefore exists that a professional member may be in breach of the Code of Ethics if he acted contrary to the privacy principles (even if he did so at the behest of his employer). It should be noted that the sanctions available to the Society's Disciplinary Committee are limited to reprimand, suspension or expulsion from Society membership (A.C.S. Constitution, Procedure in Professional Conduct Cases Instrument, Article 10). Since Society membership is not a condition of computing practice, there is no power to expel from the profession.

The A.L.R.C. considers that ". . . the sanctions provided . . . are inadequate and ineffective", but that ". . . codes of ethics . . . can fill in the gaps of general legislation . . . They can allow for informed and participatory self-regulation . . . they may sometimes be more effective at the workface than laws, because they are drawn and understood by information technology professionals rather than lawyers and legislative draftsmen" [1405].

Whether or not the Society's present Code of Ethics does in fact impose duties upon members which go beyond their employment contract, it is clear that the Law Reform Commission considers it desirable, and that the Draft Privacy Bill, if enacted, would provide a means of interpreting some of those duties.

13. CONCLUSIONS

The Commission's proposals establish for the first time, external rules against which the privacy aspects of organisational procedures may be judged. Organisations which maintain data about identified individuals especially those whose operations are dependent upon that data, should assess the likely impact of the Commission's proposals on their information systems. Computing practitioners, professional or otherwise, have important roles to play.

Acknowledgements

The assistance of Graham Greenleaf, formerly of Macquarie University and now of the University of N.S.W. Law Faculty, is gratefully acknowledged, both for reviewing drafts of this paper, and for permission to draw on portions of a joint paper presented by us to the A.N.Z.A.A.S. Conference in May, 1984. The comments of referees were appreciated, as were those of participants in presentations to the Canberra Branch of A.C.S. and the Society for Computers and Law.

REFERENCES

A.C.S. (1979): *Constitution,* Australian Computer Society, G.P.O. Box 4944, Sydney, N.S.W. 2001.

A.L.R.C. (1979): 'Unfair Publication: Defamation and Privacy' Report No. 11, Australian Law Reform Commission, Elizabeth St., Sydney, N.S.W. 2000.

A.L.R.C. (1980): 'Privacy and Personal Information', Discussion Paper No 14, Australian Law Reform Commission, Elizabeth St., Sydney, N.S.W. 2000.

A.L.R.C. (1983): 'Privacy', Report No 22, Australian Law Reform Commission, Elizabeth St., Sydney, N.S.W. 2000.

CANADA (1972): 'Privacy and Computers', Report of the Dept. of Communications and Dept. of Justice, Govt. Printer, Ottawa.

CANADA (1977): Human Rights Act, Govt. Printer, Ottawa.

CANADA (1980): 'Public Government for Private People, Vol:3, Protection of Privacy', Govt. Printer, Ottawa.

CANADA (1982): Privacy Act, Govt. Printer, Ottawa.

COUNCIL OF EUROPE (1981): 'The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', Strasbourg.

COWEN Z. (1969): *The Private Man;* Boyer Lectures, Australian Broadcasting Commission, Elizabeth St., Sydney, N.S.W. 2000.

F.O.I. (1983): Freedom of Information 1982 Annual Report, Australian Government Publishing Service.

GOLDSWORTHY A.W. (1973): 'Computers and Privacy — A Review of the Younger Committee Report' *Aust. Comput. J.,* 5, pp.3-7.

GOLDSWORTHY A.W. (1974): 'Privacy in Australia — The Morison Committee Report' *Aust. Comput. J.,* 6, pp.34-37.

GREENLEAF G.W. and CLARKE R.A. (1984): 'Database Retrieval Technology and Subject Access Principles' *Aust. Comput. J.,* 16, pp.27-32.

H.E.W. (1973): *Records, Computers and the Rights of Citizens,* M.I.T. Press.

KIRBY M. J. (1983): *The Judges,* Boyer Lecture Series, Australian Broadcasting Commission, Elizabeth St., Sydney, N.S.W. 2000.

LINDOP N. (1978): 'Report of the Committee on Data Protection', U.K. Cmnd 7341, H.M.S.O., London.

LINOWES D.F. (1977): 'Personal Privacy in an Information Society', Report of the Privacy Protection Study Commission, U.S. Govt. Printing Office, Washington.

MORISON W.L. (1973): 'Report on the Law of Privacy', N.S.W. Govt. Printer, Sydney.

NIBLETT B. (1984): 'Data Protection Act 1984' Oyez Longman, London.

N.S.W. PRIVACY COMMITTEE (1977): 'Guidelines for the Operation of Personal Data Systems: Exposure Draft', Background Paper No 31, N.S.W. Govt. Printer, Sydney.

N.S.W. PRIVACY COMMITTEE (1979): 'Employment Guidelines' and 'Employment Background Paper', Nos 39A and 39B, N.S.W. Govt. Printer, Sydney.

N.S.W PRIVACY COMMITTEE (1980): 'Five Years 1975-1980', N.S.W Govt. Printer, Sydney.

O.E.C.D. (1981): 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', OECD, Paris.

PAGANO R. (1983): 'Panorama of Personal Protection Laws', Council of Europe, Brussels.

SENATE STANDING COMMITTEE (1979): 'Freedom of Information: Report of the Senate Standing Committee on Constitutional and Legal Affairs', Australian Government Publishing Service.

SMITH R.E. (1981): 'Compilation of State and Federal Privacy Laws', *Privacy Journal* (Special Issue), Washington D.C.

STERLING J.A.L. (1984): 'The Data Protection Act 1984', CCH, London.

THOM J. A. & THORNE P.G. (1983): 'Privacy Legislation and the Right of Access', *Aust. Comput. J.* 15, pp.145-150.

THOM J. A. & THORNE P.G. (1984): 'Privacy, Technological Change and Law Reform', Tech. Report 84/9, Dept. of Computer Science, University of Melbourne.
UNITED STATES (1974): Privacy Act, U.S. Govt. Printing Office, Washington.
WESTIN A.F. (1967): *Privacy and Freedom*, Atheneum, New York.
WESTIN A.F. & BAKER M. A. (1982) *Data Banks in a Free Society*, New York Times Book Co.
YOUNGER K. (1972): 'Report, Committee on Privacy' U.K. Cmnd 5012, H.M.S.O., London.

BIOGRAPHICAL NOTE

Roger Clarke is with the Australian National University as Reader in Information Systems following 17 years in private industry in Sydney, London and Zurich. He holds an M. Com. degree from the University of NSW. His particular interests are in software development technology and social implications of computing. He was a consultant to the Australian Law Reform Commission in relation to the Commission's Privacy Reference.

Letter to the Editor

COMMENT ON THE PAPER BY MANSFIELD

I read with interest John Mansfield's article "Word? — a Paradigm of an expert system" (this journal, February, 1985). My initial interest was in the similarities — and differences — of WORD? and my own home-written version of Hangman. As I read on, however, I realized that the article was also a fine example of that old programmer's warning: Garbage in — garbage out.

First, I was pleased to find that my own program included the functions of all but one of WORD?'s sub-systems (my Hangman will not explain its reasoning). But I learnt a lot from the formal presentation of WORD? as an expert system.

Then there was the matter of GIGO. The article, including Appendix B, was written, refereed, rewritten and published. And the "expert system" still hasn't learnt to spell "cheetah". If there's one lesson to be learnt, it's that the expert system writer is not necessarily the best source of the system's expert knowledge.

Now *my* Hangman program will only accept a word after the word has been independently verified.

N. Lethbridge
Churchlands, WA 6018

AUTHOR'S REPLY

I am gratified that Mr Lethbridge "learnt a lot" from my article since that was the object of the exercise. However, I am, I confess, a little disappointed that he has categorised it as garbage apparently on the basis of a misspelt word that is part of WORD?'s vocabulary. Whilst his penultimate sentence is certainly correct that "the expert system writer is not necessarily the best source of the system's expert knowledge" WORD?'s vocabulary is derived from its use by a wide variety of students and other persons interested in expert system construction and thus reflects their erudition rather than the system writer's. The word "cheeter" was chosen merely to give a shortened example of WORD?'s pattern matching expertise.

A more serious error which I overlooked at the proof stage was the printer's inadvertent inversion of rule 14. It should read:

If: A word is successfully guessed . . .

rather than

If: A word is unsuccessfully guessed . . .

I have recently started work on an expert system to correct spelling and would welcome comments and suggestions. The system is intended to go further than the current commercial spelling checkers which inform one that a given word is not in their vocabulary.

John Mansfield
Western Australian Institute of Technology