Discussion Paper

Database Retrieval Technology and Subject Access Principles

By G. W. Greenleaf† and R. A. Clarke*

Thom and Thorne (1983) questioned the efficacy of proposed subject access to personal information because of features of relational databases. Those arguments are extended and a similar argument applied to free-text retrieval DBMS. Three sets of information privacy principles, those of the NSW Privacy Committee (1977), the OECD (1980) and the Australian Law Reform Commission (1983) are assessed against these difficulties. Weaknesses in these principles are identified. Suggestions for rationalisation of the Australian information privacy debate are made.

Keywords and phrases: right of access; subject access; individual access; data-subject access; record-subject access; privacy; data protection; freedom of information; deductive database; relational database; free-text retrieval.

CR categories: E.0, F.4, H.3, I.7, J.1, K.5.

Editor's Note: This article is in part an extended response to articles relating to privacy and computer database systems published in the previous issue of this Journal. In view of the importance of the matters raised and in the interests of expeditious publication, the normal peer review and refereeing process has been abbreviated on this occasion. The Journal will welcome other articles of this type discussing issues of current interest.

1. INTRODUCTION

The recent papers by Thom and Thorne (1983) and Bushell (1983), published in this Journal, are among the first papers published in Australia which subject information privacy principles to the type of detailed scrutiny that they deserve. The Australian Law Reform Commission's (ALRC's) *Privacy Report* (ALRC, 1983) has since been published, containing a new set of Information Privacy Principles and a Draft Privacy Bill.

Thom and Thorne raise problems involved in applying data protection principles to relational databases. We argue that similar problems arise from recent developments in free-text retrieval technology. They doubted that protection principles and regulatory mechanisms, particularly the individual access principle, are capable of adequately dealing with these problems. We examine the principles espoused by the NSW Privacy Committee (1977 and 1983) and the OECD (1980) and conclude that, if taken as a whole, and sympathetically implemented, they may be more effective than Thom and Thorne suggest. We conclude that the ALRC's principles face greater difficulties in coping with these problems.

2 RELATIONAL DATABASES

2.1 The Subject Access Principle

Thom and Thorne raise an important difficulty in defining the meaning and operation of the principle of subject access when applied to recently developed relational databases. The principle, that an individual should have access to all information concerning himself is found in some form in all known formulations of information privacy principles (see ALRC, 1983, para 1235).

The OECD (1980) refers to the "Individual Participation Principle", the NSW Privacy Committee (1977) to "subject access" and the ALRC (1983) to "Access to Records of Personal Information" and "record subjects". Because we have some reservations about the use of "records" rather than "data" or "information" (see para. 6), and for brevity, we have simply referred to "subject access", the "Subject-Access Principle", and "information subjects".

2.2 Explicit and Implicit Information

Thom and Thorne argue that the operation of this principle is reasonably clear for a database structured on a hierarchical model, but is unclear for databases structured by logic programming (relational and deductive databases, defined in Thom and Thorne, 1983, p. 146). The reason is that hierarchical databases are "accessed by a single primary key", by which we take them to mean that every record which contains information relevant to an individual will also contain a data item, the "primary key", capable of identifying that individual, and so all information concerning the individual is "stored explicitly" and can be easily accessed. In contrast to this "explicit information", "implicit information may be retrieved only by accessing and combining the information held in different records", possibly by using rules which posit relationships between data items held in different records. Deductive databases are extensions of relational databases by the inclusion of such stored rules. We use 'relational' to include both the relational and deductive models. Relational databases are characterised by the relative ease with which the stored rules enable the extraction of information stored implicitly, in contrast to the considerable difficulties encountered in manual systems or hierarchical databases.

A further distinction is made between two types of

*†School of Law, Macquarie University, North Ryde, NSW 2113. *Faculty of Commerce, University of New South Wales, Kensington, NSW 2033; present address: Department of Commerce, Faculty of Economics and Commerce, Australian National University, Canberra, ACT 2601.*
Manuscript received and revised January, 1984.

implicit information, that "which can be derived from the database using the stored rules and a single predicate query" (inferable) and that "which can be accessed only by the use of more complex queries and some external rules which are not stored as part of the database" (potentially inferable). The terms "inferable" and "potentially inferable" are ours, as Thom and Thorne do not provide any, and they use "derivable" in a different sense from our use of "inferable".

2.3 Problems with Access to Implicit Information

This discussion leads to Thom and Thorne's fundamental questions: how is implicit information included in "the information held concerning an individual" for the purposes of the principle of subject access?; and how can any regulatory mechanism hope to make a right of subject access effective in the face of such sophisticated databases?

They conclude that "the individual must have access to rules and implicit facts as well as the explicit facts" but "due to the possibly dynamic nature of rules, it may not be possible to determine all information attributable to an individual".

In illustrating these problems Thom and Thorne use an uncontentious example of a "family tree" database, but they mention the Costigan Commission enquiries (The Royal Commission on the Activities of the Federated Ship Painters and Dockers Union) as an illustration of the potential privacy dangers of the use of relational databases.

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" (Meagher, 1983a). 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. "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 of the paths between the two, even if there are several intervening persons".

The Costigan Commission is a small organisation set up to investigate the affairs of "upwards of 2,000" people and in doing so it has established a database capable of interrelating information in over 2.5 million folios Meagher's opinion is that the subject access principle "is revealing are a clear illustration of the potentially sensitive and damaging nature of such implicit information.

The ALRC has recognised that "concern might be expressed at the reach of the net that has been cast and the very large number of apparently law-abiding Australians who are caught up in that net, by reason of some association with others in activity which in most cases is probably innocent or trivial" (ALRC, 1983 para 533).

Criminal intelligence raises special problems for the operation of any data protection principles. However, Meagher's opinion is that the individual access principle "is not appropriate where the data base is being used to investigate whether that person is involved in a criminal organisation" (Meagher, 1983b p. 140). It is beyond the scope of this paper to discuss this issue (see Meagher, 1983b, pp. 87-93, 138-40; ALRC, 1983 para 533, 1418).

2.4 Latent Information

To answer "what is data relating to an individual?", we consider that as well as explicit and implicit information a further category of "latent information" must be identified and defined.

For example, consider an allegation that Smith attends the races with Jones, which information is held only in the comments field of a record "about" Jones in the sense that it is only accessible by fields containing identifiers to Jones. If the system also has no stored rules of inference concerning racing attendance or associates, Smith's involvement is not inferable. Also, the database structure or existing software may not support such potential derivation rules. For searches designed to find information about Smith, the racing attendance information is currently unretrievable ('latent') without replacement of software or database restructuring. Nevertheless, the racing attendance allegation is clearly information in the database about Smith, and is personal and potentially prejudicial. It may be discovered and used to his detriment by accident, or by exhaustive search.

We define "latent information" as information in a database which is about a person and contains an identifier to that person, but which:

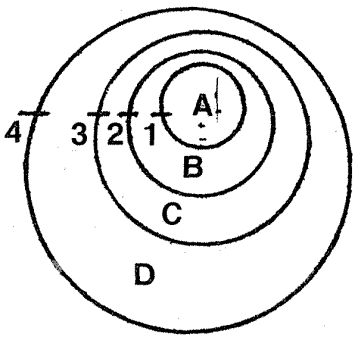
(i) is not explicit in that it cannot be accessed by use of that identifier;
(ii) is not inferable by any stored rule;
(iii) is not potentially inferable by any external rule; and
(iv) is only discoverable accidentally or by exhaustive search.

Although the dangers to privacy posed by accidental retrieval, software replacement or database redesign are less than those posed by implicit information, it is important that the existence of latent information be acknowledged as a limitation on the value of the subject access principle and other privacy protection principles. It also constitutes an important distinction between relational and free-text databases, as will be discussed later.

2.5 Categories of Database Information

We are now able to expand the categories of information which may be contained in databases beyond those proposed by Thom and Thorne by addition of the categories discussed in 2.2 and 2.4 above.

The information content of each exclusive ring comprising the database is shown in Figure 1.



A = explicit*
B = inferable
C = potentially inferable
D = latent (or non-attributable)
A+B = derivable*
B+C = implicit*
A+B+C = attributable*
A+B+C+D = total personal information in database

(Terms marked * follow Thom and Thorne)

Figure 1.

Considered from the perspective of the rules and capacities of the system allowing information retrieval, circle 1 represents the stored rules, circle 2 the external

rules (potential rules), circle 3 the structure of the software and the database, and circle 4 the distinction between information contained in the database and other information.

3. FREE-TEXT RETRIEVAL TECHNOLOGY

Free-text systems are characterised by the database over which they operate containing the full text of documents (newspaper articles, letters, telephone transcripts, court judgements), with very limited structuring of the texts during data capture, (e.g. markers to identify paragraph commencement). In this sense the texts stored are "raw data", and are in stark contrast to the data definition language used by relational and other structured databases. However, either highly structured indexes or data compaction techniques are used in conjunction with the "raw" text files.

Such databases are similar to relational databases in the use of logic as a data manipulation language. Boolean search logic, using the familiar Boolean connectors "or", "and" and "not", in combination with a variety of contextual or positional operators, allows the retrieval of all documents in the database in which a string, word, phrase or particular logically specified combination of words occurs. "There are two kinds of free-text systems: the all-software inverted file systems, and the hardware driven, associative file processors" (Stephen, 1983). The more common software products include STAIRS, STATUS and BASIS which are of general application and LEXIS which is specific to legal material. The Datafusion Associative File Processor and ICL's Content-Addressable File Storage (CAFS) are hardware examples. The differences between the two types are not of significance to this article.

3.1 Uses of Free-Text Retrieval Technology

Unstructured, discursive information has until now resisted widespread inclusion in computerised databases. The high cost of manual summary extraction and index construction constituted a *de facto* privacy protection for the extensive personal information contained in such texts. Free-text retrieval systems automate indexing or data structuring.

Until now, at least publicly-accessible databases have not included significant amounts of personal information (see Infogrow, 1982). With data capture and storage costs also decreasing, more applications involving such information will result, including:

(i) newspapers and periodicals, such as in the Australian Financial Review Information Service (AFRIS);
(ii) court reports;
(iii) criminal and national security intelligence systems;
(iv) documents of organisations which give and receive written advice e.g. policy oriented government organisations, solicitors;
(v) customer and employee records (see Clarke, 1983).

3.2 Information Privacy Problems

The ALRC has suggested nine most prominent sources of concern for privacy which have been generated by computerisation (ALRC, 1983 para 118). Consideration of these makes it arguable that widespread application of free-text systems to personal information would constitute a greater danger to privacy than any other type of database. We limit ourselves here to a consideration of the implications of relational and free-text systems for the Subject Access Principle, a matter not discussed by the ALRC.

In one sense, a free-text system facilitates subject access by a more powerful retrieval method than is available in any other type of database. An individual can search the whole database for every occurrence of his or her name or any other personal identifier, and inspect all contexts in which such occurrences occur. It makes no difference that the information may be in a record which is primarily about someone else, and there are thus no latent facts. In free-text systems, therefore, "explicit information" includes every record which contains an occurrence of an individual's identifier. This feature of free-text systems also demonstrates their potential for invasion of privacy when utilised by those other than the individual information-subject.

Although 'explicit', the information may be so discursive and extensive as to be virtually meaningless unless the information subject has some way of knowing which of it the user regards as relevant.

The distinction between explicit and implicit information made by Thom and Thorne is therefore of different significance with free-text systems. This is because every search command in a free-text system other than simple searches for every occurrence of a person's name can be said to generate "implicit information" in that the rule (the search command) must be known before what is considered to be "the information held concerning an individual" can be determined. For instance, the search may be to find all instances of "Smith" and "bribe" occurring in the same paragraph. Most information could be said to be only "potentially inferable", in that with free-text retrieval any search may involve the construction of "new rules", because the Boolean search used may be unique to the search and might not be "added" to the "stored rules", but discarded. In the extreme, there may be no "stored rules" except the handful of basic Boolean search logic rules, which are used to generate an indeterminate number of new queries. In practice, commonly used command sequences are likely to be stored in a library of procedures. Similarly, the results of any search may be used (to the subject's prejudice, perhaps) and then discarded, but the prejudicial information will remain in the database.

The resulting privacy problems are worse than for relational databases. If there are no or few stored rules, then "complex associations" may be made in a unique search, which the data subject has little hope of anticipating or duplicating. A data protection authority may also have difficulty in determining "all information attributable to an individual" when even its skilled investigators have no stored rules to work with, but just a mass of free-text and the rules of Boolean logic. There is indeed a "potential to make the right of access principle unenforceable".

These problems will be exacerbated by systems which combine features of free text and relational databases.

4. THE NSW PRIVACY COMMITTEE'S GUIDELINES

We now consider the personal data system principles of the NSW Privacy Committee (1977), to examine whether they allow access to implicit information. We argue that it isn't possible to consider the principle of subject access in isolation, without considering whether other principles may remedy the problems raised. The Privacy Committee "Guidelines" were the earliest comprehensive information privacy principles published in Australia and

the Committee announced in its 1983 *Annual Report* that "Legislation is now necessary . . . laying down privacy protection standards" and that "it is expected that any legislation adopted will codify the central principles of collection, storage, access and amendment already embodied in the Committee guidelines" (NSW Privacy Committee, 1983).

> Guideline 7. "Subject Access" states:
> "Every person should be able to know of the existence and of *the content of data* which relates to himself."
> "Personal data" is defined as "particulars concerning any characteristic of an *identifiable* natural or legal person, or the affairs of that person" (emphasis added).

Data, or at least its content, is to be accessible without qualification as to the nature of its storage (although 'uncirculated personal notes' and 'personal memory' are excluded). The data is to be accessible not only if the person to whom it relates is directly identified, but also if he is indirectly identifiable. The "Subject Access" Guideline is, therefore, arguably broad enough to require disclosure of implicit information about a person, or at least inferable information, but this is hardly clear.

> However Guideline 6, "Public Access", states:
> "The interested public should be able to know of the existence, purposes, uses and *methods of operation* of personal data systems" (emphasis added)

The principle seems to justify an information subject obtaining details of stored rules, and perhaps regularly used but still "external" rules, and thereby, of implicit information.

Another Committee policy proposes a more extensive right where a person is actually to be affected by adverse use of data about him: "before an individual is adversely affected by data he should have the opportunity for personal discussion to verify accuracy and comment on the information on which the decision is being made" (NSW Privacy Committee, 1980, p. 18). This policy seems to make no distinction between explicit and implicit information. Disclosure of reasons for adverse decisions after the decision also makes no such distinction.

5. THE OECD'S BASIC PRINCIPLES

During the period 1978-1980, the club of the 'advanced western nations', the Organisation for Economic Co-operation and Development (OECD) constituted an Expert Group to prepare a Recommendation concerning Privacy Guidelines. Although other international bodies have undertaken similar exercises, notably the Council of Europe, it is the OECD which is the most relevant reference point for Australia, particularly as the ALRC Chairman was also Chairman of the Expert Group.

The *Recommendations* of the Council of the OECD (1980) included the following principles:

> The "Individual Participation Principle": "An individual should have the right:
> (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
> (b) to have communicated to him, *data relating to him* . . ."
> "Personal data means any information relating to an *identified or identifiable* individual (data subject)"
> The "Openness Principle": "There should be a general policy of openness about developments, *practices and policies* with respect to personal data . . ." (emphasis added).

The NSW Privacy Committee Guidelines and OECD Basic Principles therefore correspond fairly closely in this area of access by the information subject. The OECD do not deal directly with the question of disclosure of reasons for decisions adverse to the data subject's wishes.

Although Thom and Thorne's conception of new problems, and our own further development of their thesis, postdate the NSW Privacy Committee and OECD proposals, their frameworks for information privacy protection appear capable of catering for the newly foreseen difficulties, if sympathetically implemented, but it could be said that this is largely due to their degree of generality rather than anticipation of the problems.

6. THE ALRC'S PROPOSALS FOR SUBJECT ACCESS

In April 1976 the Commonwealth Government referred the question of privacy issues arising under Commonwealth and Territorial laws to its Law Reform Commission (ALRC). The Commission's *Report* (ALRC, 1983), released in December 1983, deals with many aspects of privacy which are not necessarily related to information systems, including intrusive conduct and surveillance.

The ALRC (1983, para 1236), proposes ten information Privacy Principles and recommends "a right, enforceable under Commonwealth law, for an individual to have access to records of personal information held about him by record keepers". The Report includes a Draft Privacy Bill which embodies this recommendation, and includes the ten Principles as a Schedule.

We propose to discuss these Principles (see ALRC, 1983, paras 1193-1385), in isolation from their incorporation in the draft Bill. It is important to do so because the Commission's *Report* will and should become the major focus of discussion about privacy issues in this country, irrespective of whether or not the draft Bill is ever enacted, or even placed before Parliament. We will discuss the adequacy of the draft Bill in dealing with implicit information in a future issue of this Journal.

The Information Privacy Principles recommended by the ALRC draw primarily on the OECD guidelines, but their similarity to other formulations of information privacy principles is acknowledged (ALRC, 1983, para 1195, and para 638, footnote 171).

> Principle 5, Access to Records of Personal Information states that:
> "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*" (paras 1230-1277, our emphasis).
> "Personal information [is] information about a natural person from which, or by use of which, the person *can be identified*" (para 56, summarising paras 1196-1198, our emphasis).
> "A Record [is] any written document . . . [and] photographs, drawings, films, tapes and other devices for conveying or transmitting information . . . [except] . . . published documents, library material, mail and non-business records" (para 64, summarising para 1237).

We were unable to find any discussion of the novel term 'record-subject'.

There is a potentially highly significant difference between the Commission's Principles and those of the OECD because of the substitution of the term "record" for "data". "Data" (like "information") is an intangible concept, enabling the OECD Guidelines to indicate a desirable condition without concern for the manner in which the data is physically stored or communicated. A record, on the other hand, no matter how widely defined, is a tangible entity which has moreover a large number of pre-existing and specific meanings, both in the law and in computing

practice. This narrowing of the classification of accessible 'things' may be the cause of the difficulties discussed below.

The ALRC acknowledges that "Freedom of Information legislation, untrue to its title, is generally framed in terms of access to *documents* (however defined) rather than access to *information*" (ALRC, 1983, para 1407, emphasis in original) but does not discuss any implications that a parallel shift from the intangible to the tangible may have for its information privacy principles and their operation.

The ALRC's motivation in using the term 'record' is clear: "every effort should be made to ensure the compatibility between the entitlements . . . under both the Freedom of Information and Privacy Acts" (ALRC, 1983, para 1408). That this consideration should be given weight in the preparation of the Draft Privacy Bill is undoubted, but we doubt its merit in the formulation of the general principles.

A further significant discrepancy between the OECD and ALRC Principles is the absence in the latter of any Openness Principle. Consequently, there can be no argument for access to stored rules based on such a principle. Principle 2(c) does require disclosure by the record-keeper, at the time of information collection, of "his usual practices with respect to disclosure", but this seems to have little relevance here. We are unable to find any explicit statement in the Report as to the reason for this important omission. It could be that the Commission has assumed that the Openness Principle is one of freedom of information, not privacy, or that the *Freedom of Information Act 1982* has already implemented that principle. Our view is that if openness concerning such aspects of system operations as the existence of stored rules is necessary for adequate privacy protection, then such a principle should be part of a comprehensive set of Information Privacy Principles *as well as* part of Freedom of Information principles. If not, then in those areas where Freedom of Information has no application, the Information Privacy Principles will be incomplete and misleading.

> The *Freedom of Information Act*'s objects are:
> ". . . to extend . . . the right . . . to access to *information in the possession of the Government of the Commonwealth* by –
> (a) making available to the public information about the *operations* of departments and public authorities . . .; and
> (b) creating a general right of *access to information in documentary form*" . . . (*Freedom of Information Act 1982*, Section 3, emphasis added).

The reference to 'documentary form', is somewhat limiting and the focus of 'operations' is narrower than the OECD's 'developments, practices and policies'. The main deficiency is, however, that the scope of Freedom of Information is restricted as yet to the public sector. The Commission asserts that its "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" (para 1409), but we can not find any such proposals beyond the individual access provisions. This means that the ALRC makes no allowance for individuals to discover 'stored rules' or 'implicit information' by requiring that private sector organisations disclose their practices and policies.

The Commission makes no reference to the question of the communication to data subjects of the reasons for adverse decisions. They did however give consideration to the need to introduce a general requirement that where such decisions were made the person should be notified of the decision and of their rights including inspection of the "relevant record". While regarding this as "thoroughly desirable as a good administrative practice", they deferred the matter for future re-consideration (ALRC, 1983, para 1397). This would in any case fall short of the Privacy Committee's proposal that the person should be able to "comment on the information on which the decision is being made" and the emphasis on access to records may again exclude access to stored rules and implicit information.

One intriguing future possibility raised by the ALRC (1983, para 1406) is that of "direct access by a record-subject to the terminal to interrogate the information base and thereby to secure access to the required information". Such access would clearly be limited without access to at least stored rules.

7. A NEW STAGE IN THE AUSTRALIAN INFORMATION PRIVACY DEBATE

7.1 Confusion Over Principles

A major problem in the information privacy debate which has smouldered in Australia for over a decade is that it has suffered from a number of competing sets of principles being advocated. As Bushell (1983) points out, confusion has arisen in South Australia, where as late as June 1983 the State Government's Data Processing Board issued a set of interim principles which bore little relationship to those under discussion elsewhere. This is even more confusing than Bushell states because in doing so the South Australian Government was ignoring the recent recommendations of its own Law Reform Committee (SALRC, 1980) that the recommendations of the UK Lindop Committee (Lindop, 1978) be substantially adopted.

The problem is not that different principles, or different methods of implementation, are being advocated, but rather that the debate has been carried on with too little common structural framework. When developed in full, general principles of information privacy comprise many sub-principles or exceptions and are inter-related at many points. They are designed to deal with an enormous variety of information systems, and many aspects of a full set of principles will only be relevant to some types of systems. Different approaches to such principles can only sensibly be compared point by point to determine where overlaps, differences and omissions occur. Such comparison, and resulting informed debate, is greatly facilitated if competing principles are constructed on a common framework.

Differing terminologies are just as confusing as differing structures. When differing principles use "data", "information" or "record", it is often difficult to know whether real distinctions are being made, and comparisons are difficult.

7.2 1984: A Brave New World?

The ALRC *Privacy Report* (1983) brings a new stage in this debate. The Information Privacy Principles recommended by the ALRC have broad similarities to previous proposals. We have criticised some aspects of the ALRC's Principles, and a fuller consideration of all the ALRC's Principles and the draft Bill is obviously necessary.

The ALRC proposals are supported by more extensive argument and documentation than previous proposals. In our view, the principal item on the agenda of the Austra-

lian information privacy debate should be for all the parties to that debate to determine whether the ALRC Information Privacy Principles provide an adequate framework and terminology. If there are reservations about the precise content of different principles, or the best method of implementation or enforcement, that does not matter so much if the participants are working within a common framework, and their differences are thus identifiable and debatable. If, of course, the ALRC framework or terminology is regarded as fundamentally inadequate, then it should not be accepted. Perhaps ACS could take the lead and consider whether the ALRC Principles (or some modification of them) should be adopted in substitution for its own privacy principles (see ACS, 1982).

REFERENCES

ALRC (1983): The Law Reform Commission, *Privacy*, Report No. 22, Australian Government Publishing Service (AGPS), Canberra, 920 pp + microfiche.

ACS (1982): *Privacy* Position Paper No. 1, Australian Computer Society, Sydney.

BUSHELL, C.J. (1983): Privacy Versus Policy, Precedent and Expediency, *Aust. Comput. J.*, Vol. 15, No. 4, pp. 151-3.

CLARKE, R. (1983): Modern Marriage By Info-Text, *Aust. Computerworld*, 1 July 1983.

Infogrow (1981): *The Infogrow Australian Database Directory*, Infogrow (Aust) Pty Limited, 49 Clarence St, Sydney.

LINDOP (1978): *Report of the Committee on Data Protection*, Cmnd 7341 HMSO London.

MEAGHER, D. (1983a): Computer Use by the Costigan Commission, *Law and Technology Seminar Papers*, Vol. II, Brisbane, Qld., August 1983.

MEAGHER, D. (1983b): Paper IV, Gathering Information and Paper V, Management of Information, *Organised Crime*, AGPS, Canberra 1983 (Papers presented to the 53rd ANZAAS Congress, Perth, Western Australia, May 1983).

NSW Privacy Committee (1977): *Guidelines for the Operation of Personal Data Systems*, Privacy Committee, Attorney-General's Department, Box 6, GPO Sydney, 27 pp.

NSW Privacy Committee (1980): *Five Years 1975-1980*, Privacy Committee, Attorney-General's Department, Box 6, GPO Sydney.

NSW Privacy Committee (1983): *Annual Report 1982*, Privacy Committee, Attorney-General's Department, Box 6, GPO Sydney.

OECD (1980): *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development, Paris.

SALRC (1980): *Fiftieth Report Of The Law Reform Committee of South Australia Regarding Data Protection*, the Committee, c/- Supreme Court, Victoria Square, Adelaide.

STEPHEN, C. (1983): Computerised Legal Information Retrieval in Australia, *Law and Technology Seminar Reports*, Vol I, Law and Technology Committee, Brisbane, Qld., August 1983.

THOM, J.A. and THORNE, P.G. (1983): Privacy Legislation and the Right of Access, *Aust. Comput. J.*, Vol. 15, No. 4, pp. 145-50.

BIOGRAPHICAL NOTES

Graham Greenleaf, currently tutor in the School of Law, Macquarie University, received Arts and Law degrees from the University of Sydney in 1975. He subsequently undertook legal research and was engaged in private practice. He is foundation President of the New South Wales Society For Computers And The Law. His research interests include information law, privacy and property law.

Roger Clarke has recently joined 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.

The two authors were Research Officers for the NSW Privacy Committee in 1975-1978 and 1976-1977 respectively, and were closely involved with the drafting of the Committee's information privacy guidelines.