PRIVACY COMMITTEE

GOODSELL BUILDING
8-12 CHIFLEY SQUARE, SYDNEY
BOX 6 G.P.O., SYDNEY. N.S.W. 2001
TELEPHONE: 238 7713
REF. R.A.C.

B.P. 31

EXPOSURE DRAFT

April, 1977.

GUIDELINES FOR THE OPERATION OF PERSONAL DATA SYSTEMS

These guidelines have been provided to assist organisations using information about persons, to ensure that their practices do not unduly intrude upon those persons. They were prepared after eighteen months' experience by the Committee, including the investigation of a wide variety of complaints and study of a number of Personal Data Systems in both the public and the private sectors.

Further papers will be published by the Committee as companions to this set of Guidelines. One will privide a discussion of the justification for each particular guideline, another will summarise relevant overseas proposals, and a third will summarise the guidelines for the general public.

In addition, sets of guidelines have been and will be issued relating to specific types of system, e.g. credit bureaux, criminal records, medical data, employment files.

All system operators are invited to examine these guidelines, implement the provisions voluntarily, and provide the Committee with comments and criticisms on their practicality, effectiveness and cost. Similarly, persons and organisations concerned with privacy and civil liberties are invited to submit their comments and criticisms.

The Committee will then publish firm Guidelines. For a period of two years it will observe the Guidelines in practice, and deal with complaints the parties have been unable to resolve. Consideration will then be given as to whether it should recommend legislation of some or all of the Guidelines in relation to some or all operators of personal data systems.

Submissions should be addressed to the N.S.W. Privacy Committee, G.P.O. Box 6, Sydney 2001. Verbal comments will also be acceptable; 'phone (02)2387713. Submissions should reach the Committee by 30 September, 1977.

1. INTRODUCTION.

1.1 Who are the Guidelines For?

The Guidelines are relevant to all managers and government officers who, in the performance of their functions, use personal data. They are also relevant to specialist data processing people like Records Officers and E.D.P. Managers.

By personal data is meant particulars concerning any characteristic of an identifiable natural or legal person, or the affairs of that person.

A personal data system is a collection of data files and procedures which collects, stores, processes and/or disseminates personal data.

The Privacy Committee studies the impact on privacy of a wide range of practices. In all of its work it strives to assist society to find a fair balance between, on the one hand, the need for personal privacy, and on the other, various social and economic requirements.

These guidelines seek to establish a framework which will assist organisations to achieve their legitimate aims without undue intrusions into people's lives.

The guidelines relate to both the private and the public sectors and to both manual and computerised systems.

Clearly the importance of particular guidelines, and the cost and administrative difficulties of different methods of implementing them, will vary considerably between systems. More specific sets of guidelines will be developed in particular industries (e.g. credit, banking, insurance), in particular functions (e.g. employment), and in particular public service areas (e.g. criminal records, health records).

The Committee actively encourages all organisations to increase their staff's awareness of the privacy problems that arise out of commercial and governmental activity. Similarly the importance of professional ethics and industry codes of conduct is recognised.

1.2 What's in the Guidelines?

2. THE SEVEN BASIC PRINCIPLES.

These are intended to guide organisations in achieving their legitimate aims without undue intrusion into people's lives. In different situations different methods of implementation of these guidelines will be appropriate.

3. THE DETAILED GUIDELINES.

The Guidelines are in three sections dealing with the justification for the system, the system's operation, and the mechanisms of public access.

A. THE JUSTIFICATION FOR THE SYSTEM.

The first two guidelines are concerned with the justification (or the 'raison dêtre') of the system. They therefore deal with its purpose, and the uses to which it is put.

(1) SOCIAL ACCEPTABILITY OF THE SYSTEM'S PURPOSE AND USES.

General Principle: A personal data system should exist only if it has a general purpose and specific uses which are socially acceptable.

By 'general purpose' of a system is meant the most abstract statement of objectives, e.g. in relation to a driver licensing system, "the administration of motor vehicle licensing in N.S.W."

By 'specific uses' is meant the operational objectives implied by the very general 'purpose',

e.g. "identification of licensed drivers;
sending out of renewal notices;
collection of licensing fees; ..."

Social acceptability is not synonymous with 'legality' since some unacceptable forms of behaviour may be legal but not socially approved. The question of what constitutes 'social acceptability' is clearly not a simple matter. Discussion by the general public, by the public's elected representatives, and by the media will provide guidance. The Privacy Committee has a responsibility to stimulate debate and provide background information on important issues.

This paper does not attempt to define what purposes and uses are and are not acceptable. In specific instances the Committee will be pleased to discuss this matter with any person or organisation.

The system operator must be clear as to the purpose and uses of the system because many eatures of the system must be judged against its purpose.

(2) RELEVANCE AND SOCIAL ACCEPTABILITY OF DATA FOR SPECIFIC DECISIONS.

General Principle: Personal data should only be used when it is relevant to the particular decision being made, and its use for this decision is socially acceptable.

(a) Relevance. By this is meant the existence of a demonstrable relationship between the decision or determination being made, and the particular item of information. The decision-maker should be able to justify his need for the information on the basis that depending on the answer, different decisions might be made.

Two special cases arise:

(i) Compulsorily Relevant Data. In some situations there may be legal or social responsibilities which make certain information compulsorilly

Guideline (2)(a)(i) continued.

relevant to a particular decision. For example, since the old-age pension is subject to a means test, interviewers must ask questions concerning income and assets; under the Money Lenders and Infant Loans Act a spouse's permission is required for some kinds of loans; and a professional body (e.g. of engineers) must clearly ask questions about qualifications when considering an application for membership, since it recognises a responsibility to protect society from unqualified persons.

In most situations such factors do not arise, and decision makers may reasonably use such information as they may fairly acquire, and whose relevance they can demonstrate;

(ii) Age of Data. In general information about the distant past is not as relevant as more recent information, since it is less likely to help in assessing current or future worth. For example, the credit industry in assessing an applicant for finance, aims to assess the person's current and future credit-worthiness, not what it was in the past. For this reason credit records over five years old are not generally regarded as of much value. Similarly employers rarely seek detailed employment histories beyond about ten years; and old criminal offences, especially minor ones, are less often considered of importance by employers and licensing authorities.

This is of great importance to many people, since it provides a very real opportunity for those with a once-bad record to make a fresh start.

(b) Social Acceptability. In some circumstances even though the information is relevant, its use in certain decision-making situations may be prohibited by law or be socially unacceptable. This is the intent of racial and sex anti-discrimination provisions and some criminal rehabilitation proposals. Community standards also largely preclude questions on religious and political affiliations.

The reason for such prohibition is the sensitivity of the data, by which is meant the importance which a given person places upon the non-disclosure of a given item of information.

It should also be recognised that some individuals will be acutely sensitive about particular items of information, usually for reasons that are not apparent, and which are often thoroughly irrational. Organisations should be prepared to handle such exceptional circumstances with human understanding, e.g. the rejection of an application form because a person declines to answer one minor question will frequently be unreasonable.

B. THE OPERATION OF THE SYSTEM.

This group of three guidelines is concerned with what goes on in the day-to-day operation of personal data systems. The reasonableness of the features of any system must of course be assessed in the light of the system's justification, as discussed in Guidelines (1) and (2);

It is stressed that the term 'system operator' is used to refer to the person or organisation by whom or on whose behalf the system is operated. The responsibility is only secondarily that of records officers and data processing managers; the prime responsibility is vested in the 'user', the manager who himself or through his staff operates the system.

(3) DATA COLLECTION.

General Principle: The minimum necessary data should be collected, using fair collection methods, and from appropriate sources.

(a) How much data should be collected:

(i) in general the minimum data necessary to achieve the purpose is all that should be collected. Speculative collection, on the grounds that it may be needed later and would be more economically collected now, should be avoided;

(ii) adequate identification data should be collected to make the association of data with the wrong person highly unlikely. In a small file, the person's full name and/or file or account number may be adequate. In larger files the person's suburb of residence, or postcode, and in very large files, (i.e. several million) even date of birth, may be necessary;

(iii) data should only be collected if it satisfies the criterion of data relevance. (See Guideline (2) above).

Unless it can be demonstrated that information will be relevant to a future decision it should not be collected;

(iv) serious consideration should be given as to whether some sensitive classes of information should be collected at all, even if demonstrably relevant, e.g. suspicion of crime, dismissed charges, political and religious beliefs, sexual habits and race should only be sought where the need is a most important one.

(b) Collection From the Individual.

Wherever possible, data should be collected from the person himself. This avoids people taking unnecessary inferences that the organisation distrusts him and is working behind his back.

(c) Collection Procedures:

(i) the collector's identification and affiliation should be clear to the person so that he is in no doubt who has collected the information from him;

(ii) the collector should take appropriate steps to ensure the person is aware of the purpose and uses for which the data is collected. This is particularly important when sensitive information is sought, such as medical, financial and criminal details and racial origin.

Where the uses are those which the person should reasonably infer from the relationship, and no others, then the collector may need to do no more than be ready and willing to answer questions;

(iii) the collector should not use improper practices such as deception or trickery to collect information. For example it is not acceptable for a private investigator to pose as a friend of a woman's deceased husband, since this creates an unjustified assumption of a friendly relationship;

(iv) the person should be able to readily ascertain:

- the consequences if he refuses to supply the data; and

- the method whereby he may direct an enquiry or complaint.

In some cases it may be appropriate to advise this automatically, in others only if the person asks;

(v) where the person may be compelled to supply the information, the authority for the demand should be advised to him. Frequently this will only be necessary if he at first refuses.

(d) Collection from a Third Party:

(i) Data about a person should only be collected from from a third party when there is a demonstrable need to do so. The major classes contemplated are:

- where the person himself does not know, e.g. a medical report;

- where the person himself has a vested interest and/or a bias, and the information is important, e.g. the comments of a previous employer, documentary certification of qualifications, ownership of real property, etc.;

- where it is clearly economically prohibitive to collect from the subject.

- where there is legal compulsion to collect from a third party (e.g. Taxation Department must receive group certificates from employers under S221F(5)(f) of the Income Tax Assessment Act).

(ii) Where data about a person is collected from a third party the person's consent should be gained first. It is preferable that such consent be explicit, but in some cases the nature of the relationship may be such that consent is implied.

An exception exists where the operator has legal authority to collect the information, in which case the operator should take reasonable steps to ensure the person knows in advance that the information will be collected.

For example many licensing authorities access applicant's criminal records in order to assess their fitness to hold a licence. It seems appropriate for such authorities to be open with the applicant about their practices.

(iii) Where data about a person is collected not from a personal data system but from an individual's memory or personal documents, the person's consent should be gained first. If consent is not first gained, then (iv) below assumes even greater importance.

(iv) Where data about a person is collected from a third party, and is sufficiently adverse to influence the decision against the person's interests, the content of the information should be communicated to the person prior to an adverse decision being made. This provides a check on the accuracy of the information, enables discussion as to any further relevant factors, and makes clear to the person what led to the adverse decision.

There will be some circumstances in which this will be in breach of what the provider believes to be a confidence (e.g. currently some references from educational institutions and bankers). It appears from overseas experience that in few circumstances does openness preclude frank comment, and the Committee invites all system operators who wish to protect information collected from a third party to contact the Committee and communicate to us the justification for the protection.

(v) Where the content does not make sense without knowing the source, then the source should be disclosed also. Where this is not the case, it is less important that the source be advised to the person. The Committee nonetheless encourages openness except where a real fear of reprisal against the informant exists.

(4) DATA INTEGRITY, SECURITY AND RETENTION.

General Principle: Standards should be established and maintained regarding data integrity, data security, and the period for which identified personal data is retained.

(a) Data Integrity.

By this is meant the fairness with which the information represents some factor about the person. This is influenced by the accuracy, the timeliness and the completeness of the information.

(i) Accuracy.

By this is meant the close correspondence between the information recorded and the facts. The following features will generally be desirable from the viewpoint of the organisation as well as that of the data subject:

- protection against corruption.

Corruption involves the unjustified changing of data between the time it is collected and when it is accessed. It can result from bad hand-writing, smudged typing or carbon, poor quality photo-copying, bad keypunching, programming error, computer hardware error, electrical interference, intervention by a staff-member, etc. Appropriate forms of protection will vary between circumstances;

- protection against wrong identification.

This involves the association of descriptive data with the wrong person, making two persons' files incorrect, one through the absence of relevant data and the other through the presence or irrelevant data. It can result from inadequate identification data on the file, or on the new data, bad hand-writing, bad keypunching, programming error, computer hardware error, etc. Appropriate forms of protection will vary between circumstances;

- adequate differentiation.

This involves the recording of data in such a way that the meaning does not become confused with other similar meanings e.g. in hire purchase record-keeping a repossession of a vehicle must be differentiated from a voluntary surrender, because even though much of the activity which follows is identical, the impact on the borrower's creditworthiness is quite different. Similarly under s.556A of the Crimes Act, 1900 the Court may find the facts proven, but due to the person's character, or the circumstances, may not proceed to a conviction. This should not be recorded as a conviction, but either as a separate type of entry, or on another file entirely.

Commonly, errors of this kind are a result of coding systems which do not contain sufficient alternatives;

Guideline (4)(a)(i) continued.

- caution with opinions and value judgments.

  Where a suitable objective measure is available this should be preferred to a subjective one. By this is meant that a fairly precise comparison against a known scale (e.g. "Mr. X. has been over 21 days late in payments on three occasions in the last 12 months") is preferred to a vague comparison against an unknown scale (e.g. "Mr.X. is a slow payer").

  In addition, the source and date of opinions should be recorded with the data, to enable anyone using the data to have some appreciation of the context in which it was given, especially its age;

- ability to verify.

  adequate documentation should be available to enable any future queries or disputes to be resolved. Where this is not the case and the data's accuracy is challenged, the operator should delete or suitably notate the data. See also Guideline (7) on Subject Access.

(ii) Timeliness

By this is meant the absence of unreasonable lag between the occurrence and the recording of it by the system. That is to say the file should be updated with the new data sufficiently early so that users of the system are not misled.

The standard of timeliness will vary depending on the nature of the system. For example, advice of change of address often does not need to be actioned immediately, provided it is done before the name and address is next accessed. On the other hand a file of the names of people for whom arrest warrants are outstanding, or of vehicles advised as stolen, must be updated as soon as possible to avoid wrongful arrest and the embarrassment, unpleasantness and even violence that can follow if a person is wrongfully arrested.

(iii) Completeness

By this is meant the avoidance of a particular piece of data being used without other data which is related to it in an important way. For example the information that a person was late in paying a number of instalments on a finance contract would be incomplete if it was not also noted that the person had been unexpectedly hospitalised. Similarly advice by the Courts to some statutory bodies of charges against their members without subsequent advice of the result of the hearing, is an example of incompleteness.

A special case of completeness is the recording of an appeal lodged against a specific decision, since in this case a subsequent decision can in fact cause an amendment to existing information rather than addition of new data.

Guideline (4) continued.

(b) Data Security.

By this is meant the precautions taken against unauthorised access to and use of information. (Note that the term is sometimes used more broadly to refer also to measures taken to ensure what is called in this paper "data integrity").

In general the level of security should be commensurate with the data's sensitivity. There seems to be considerable argument at times about which data are sensitive and which are not. As a guide such matters as political and religious affiliations, sexual activities, criminal record, medical history, racial origin and financial details are amongst the most sensitive data. Date of birth, place of abode, family details and marital status (as distinct from title used), are also regarded as sensitive by some.

Security precautions are needed from the time of collection of the data right through until its deidentification or destruction.

The types of physical and procedural measures available are dealt with in specialist books on security. Depending on the type of system, advice and publications are available from the Australian Institute of Chartered Accountants, the Society of Accountants, the Chartered Institute of Secretaries and Administrators, the Australian Computer Society, and the E.D.P. Auditors Association.

It must be recognised however that no security measures are foolproof. The data is always at risk, and security procedures alone will not guarantee data subjects that they will be free from privacy invasions.

(c) Data Retention.

Identified personal data should only be retained for as long as a use remains.(See Guideline (1) regarding socially acceptable uses).

It should then be either:

- destroyed;

- deidentified, if the raw data has or may have some statistical research value; or

- archived, if the data has historical or research value which is of greater importance than the potential privacy problem the data represents. Archived data should not be accessible in the same manner as 'live' data, and should be subject to additional security measures at least during the person's life.

In some cases it may be appropriate to decide in advance of collection how long the data will be retained, and perhaps also to communicate the planned retention period to the subject.

(5) DATA ACCESS.

General Principle: Personal data should only be accessed consistently with the system's socially acceptable uses and for additional uses by consent or by law.

By 'access' is meant any type of communication of data maintained within the system, to any person or organisation.

For convenience, this paper will use the terms 'internal access' when the recipient is a person within the system operator's own organisation; and 'external dissemination' when the recipient is outside the organisation. Further comments on the distinction between the two terms are contained in Section 6.

(a) Fair Access to Personal Data.

The following four classes of access are fair:

(i) accesses which are implied by and consistent with the system's socially acceptable uses. (See Guideline (1) for comments on social acceptability.)

While this covers access by some staff-members and in a few cases persons external to the organisation, it only does so when they have a need for the data which is related to the system's purpose;

(ii) other accesses to which the subject of the data has given consent. For example a patient's authority is necessary for a doctor to send a medical certificate to the person's employer. Similarly a courier should not have access to the message he is carrying unless he has the consent of his client.

Consent must always be informed, by which we mean that the person giving it must have a reasonable understanding of its implications. In particular a general authorisation by an applicant for employment or insurance, for the company to approach any doctor or hospital for any information about him, is not informed since he has no means of knowing how, when and for what particular reason the authority will be used. Specific consent should be acquired, and brought to the notice of the organisation from whom information is sought.

Consent cannot be given under physical or psychological duress, by which we mean a threat of some kind. For example a refusal to supply medical services unless the person was prepared to supply certain information for a research project, would preclude a real consent being given. Refusal to supply goods or service would not generally constitute duress except where an effective monopoly situation existed.

Just because the subject requests or consents to the access does not necessarily mean the access should take place; the operator may have an interest he may reasonably wish to protect;

(iii) other accesses which are legally authorised, including legislation, regulations, by-laws, and official rules; and also approval of a legally-empowered body. The justification for all such laws is of course always subject to review;

Guideline (5)(a)(iii) continued.

A number of circumstances exist whereby a Government Agency can demand information from a company or department about a particular person. For example, the Taxation Department under s.264 of the Income Tax Assessment Act, the Department of Social Security under s.141 of the Social Services Act, the police by warrant, and Courts by subpoena. The organisation providing the information should take all reasonable steps to ensure the person is advised the information has been provided, unless the law specifically requires this not be done. The Committee knows of no such law.

(iv) emergency uses, where the failure to allow access is likely to be a significant factor in serious physical or emotional harm occurring to some person

In all cases of emergency access, the operator must subsequently ensure that an appropriate person or organisation (commonly the data subject) knows that the access occurred, so that they may complain if they think it was improper.

This justification for access should not be lightly used. The Committee is most concerned that it does not become a convenient way of circumventing the other protections in this Guideline.

(b) 'Commonly Accepted' Accesses.

There are some forms of access which do not fall into any of the above classes of fair access. The claim of parties using such arrangements has been that the access has some economic or social benefit, and that complaints are rare.

However most arrangements of this kind are relatively little known, particularly amongst the classes of persons who might be opposed to them. Therefore the claim that complaints are rare may be spurious.

The Committee intends to progressively assess each such arrangement in existence in N.S.W., where necessary seeking public comment on its effectiveness and intrusiveness. Where appropriate such access will be given approval, and so become a fair practice under (a)(iii) above.

Internal access arrangements of this nature which have come to the Committee's notice are:

- the use by a hospital of patient data to contact potential participants in a research project;
- the use by a company of one operating division's customer list to advertise the products or services of another division; and
- the monitoring by a trading bank of the organisations with whom its customers do business in order to advertise the bank's travel services.

External disseminations which the Committee has under review are:

- the sale of driver licence and motor vehicle registration details by the Department of Motor Transport;
- the sale of 'mailing lists';

Guideline (5)(b) continued.

- the provision of information by credit grantors to credit bureaux;

- the interchange of information, between Government Departments which exercise regulatory power over individuals and corporations.

The Committee wishes to be advised of all arrangements of this kind.

(c) Conditional Access.

Where a system operator provides identified personal data to another person or organisation, it will often be appropriate to nominate the specific conditions under which it is provided, and to enforce those conditions. For example:

- the Department of Motor Transport provides weekly lists of new vehicle registrations to the automotive manufacturing industry under conditions which limit the use for canvassing sales;

- credit bureaux within N.S.W. provide reports to credit grantors on the condition that applicants who are denied credit as a result of the report are given a standard letter advising them so, and enabling them to check the contents of their record;

(d) The Recipient of the Information.

If the recipient of the information stores it in his own personal data system, then the whole of these Guidelines are relevant to his system. The organisation providing the data should therefore ensure he is aware of the Guidelines' existence.

(e) The Recording of Accesses:

(i) Recording. In some circumstances the fact that information was accessed should be recorded by the system operator. This is particularly the case in systems which store sensitive personal data, e.g. medical and social case notes; credit bureau reports; and legally authorised accesses by taxation, social security, police and court officers.

These records of accesses may need to be retained until the record itself is de-identified or destroyed.

(ii) Advice to Subject of Accesses. In circumstances where accesses to sensitive information are recorded, reasonable steps should be taken to ensure that the person knows that information has been disclosed about him. In some situations it will be appropriate to advise the person automatically, but in others only if the individual asks. This 'open dealing' should largely overcome public fear of what 'they' or 'the bureaucracy' can find out without the citizen's knowledge.

The frequency of and reasons for such disclosures should also be publicly available.

(iii) Advice to previous recipients of the data. In some circumstances if data is corrected,

Guideline (5)(e)(iii) continued.

> deleted or has other data added to it for completeness, the change should be notified to recent recipients of the data. For example, amendments to credit bureau reports following subject access and challenge may need to be advised to anyone who received the data within the last six months.

This paper does not attempt to define which systems should and should not incorporate recording of accesses. In specific instances the Committee will be pleased to give its views.

C. MECHANISMS OF PUBLIC ACCESS.

The last two guidelines are concerned with the openness of dealings between the system operator and the interested public, in particular the persons about whom information is recorded.

(6) PUBLIC ACCESS.

General Principle:

The interested public should be able to know of the existence, purpose, uses and methods of operation of personal data systems; to object to any feature of a system; and where appropriate to have change enforced.

By the 'interested public' is meant those members of the public who have a demonstrable interest in the system, or who represent one or more members of the public who have a demonstrable interest. In particular this includes data subjects, and persons who may become data subjects.

Much of the fear which exists about 'databanks' does so because people think there are secret systems which store 'who-knows-what?' about them and distributes it to 'who-knows-where?'. This fear, which is frequently without grounds, is unfortunately fuelled by both public and private sector reticence about the systems they operate.

Four points are discussed:

- public knowledge of the system's existence and purpose;
- public knowledge of the system's uses and methods of operation;
- public objection; and
- public challenge and enforcement.

(a) Public Knowledge of the System's Existence and Purpose.

There should be no attempt to conceal the fact that the system exists. Any question from the public about its existence and general purpose should be answered clearly. This applies to all systems, including those which for important reasons may require a measure of protection from the public gaze, e.g. national security and criminal intelligence files.

Some governments overseas have required all systems operators to publish annually the existence of their systems (e.g. U.S. Federal Government Agencies), or to register their systems with a government agency (e.g. Sweden for both public and private sector, and probably shortly the U.K. also). These seem to the Committee to be expensive solutions to a problem which can probably be overcome quite effectively much more cheaply, by acceptance of this guideline.

(b) Public Knowledge of the System's Uses and Methods of Operation.

With few exceptions the system operator should answer questions from the public about any aspect of the system.

Guideline (6)(b) continued.

Two types of exception are accepted:

(i) where the volume of requests or the detail requested becomes prohibitively excessive.

To date the Committee knows of no occasion in Australia or elsewhere on which the adoption of a policy of 'openness' has led to prohibitive levels of use. However it is possible that an activist group or a section of the media, could place an organisation in a state of siege; or a person could seek to exploit this privilege for the purpose of acquiring commercially valuably information;

(ii) where the purpose of the system would be seriously prejudiced by publication of the system's features, and the importance of the system outweighs the privacy problem so generated. This exception will mainly include national security and criminal investigation files.

Even where these exceptions arise a method of achieving public knowledge is still necessary. Section 4 below contains the Committee's proposed method in such situations.

(c) Public Objection.

Where a member of the public opposes some feature of a system, he should have a means open to him whereby he can express his objection.

It is most important that organisations have complaints mechanisms to handle such objections. Many major disputes can be avoided if the complainant receives a hearing from a reasonably senior staff-member, and, where he remains dissatisfied, is given a clear indication of the organisation's view, preferably in writing.

Although this will undoubtedly involve effort and expense, the Committee can see no evidence that the effort and expense will be prohibitive. The benefits in terms of public confidence in its institutions will be considerable.

(d) Public Challenge and Enforcement.

Where a member of the public is opposed to some feature of a system, there should be an avenue available to him whereby he can seek to have a desired change enforced by a suitable authority.

No ground presently exists whereby a member of the public can himself request the Courts to enforce change of any practice. A complaint can be made to the Privacy Committee which has the power to investigate, and to make recommendations to the organisation concerned.

At some time in the future, with more experience of the extent to which such problems actually arise, the Committee may find it necessary to recommend the creation of some such ground. In the interim it is felt that the measures outlined below in Section 4 are adequate.

(7) SUBJECT ACCESS.

General Principle: Every person should be able to know of the existence, and the content of data which relates to himself; to complain about any feature of that data or its use; and where appropriate to have change enforced.

A major source of concern by the public about 'databanks' arises from people's inability to find out what is on file about themselves, or to correct what they regard as erroneous information.

The term 'data subject' is used to refer to the natural or legal person to whom the data relates. It may therefore refer to a human, or to a company or an association.

In addition to having a responsibility to deal with data subjects, a system operator should also deal with any representative or advocate the person nominates. This might, for example, be his local Member of Parliament, his solicitor, his doctor, the Privacy Committee, or some friend or relative he feels is more articulate than himself.

Where a legal guardian exists (e.g. minors and seriously retarded adults), then in general the guardian should be accepted as exercising the data subject's privileges. There may be some exceptions to this however, particularly the medical, educational and social welfare files of children in the transition period to adulthood (e.g. 14-18 years).

In the case of a deceased person, his Executor or Administrator or if one is not appointed then his next-of-kin, should be accepted as acting on his behalf.

In addition, a small number of circumstances exists where some of the measures outlined in this Guideline may need to be exercised by or with the assistance of some other party nominated not by the data subject but by law or by the system operator. This party is referred to as an 'intermediary'.

Five points are discussed:

- subject knowledge that the system operator holds information about him;
- subject knowledge of the information held;
- subject knowledge of accesses;
- subject complaint; and
- subject challenge and enforcement.

(a) Subject Knowledge That the System Operator Holds Information About Him.

There should be no attempt to conceal from a data subject that information is held about him; the system operator should answer clearly any such question. This guideline is vital since other protections of the individual's privacy may be negated if the person is unable to know that information exists about him.

Guideline (7)(a) continued.

Some Governments overseas have required the system operator to advise the data subject when a file is created (e.g. U.S. Federal government agencies), and even to advise the person on each occasion when new information about him is acquired from a third party. These seem to the Committee to be expensive solutions to a problem which can probably be overcome quite effectively much more cheaply.

(b) Subject Knowledge of the Information Held.

In general the system operator should on request permit a data subject to have access to the data on file about himself. In a few cases it may be appropriate for this access to be permitted not to the data subject, but to an intermediary.

There are three types of exception:

(i) Where the data may in itself be harmful to the subject. In such cases (which will mainly arise with psychiatric and some other medical files), it is reasonable for the person to be given a suitable non-detailed explanation. In the event that he insists on having personal access, denial will probably be more harmful than the alternative, and access should usually then be permitted.

(ii) Where the data is likely to be misinterpreted by the subject, with likely harmful effect. This occurs in files which contain a substantial amount of:
- technical jargon;
- abbreviations and shorthand;
- terse comments which depend on the technical context for their full meaning.

In such situations (which will often arise in medical record-keeping), the subject should be permitted access only with the assistance of a suitably qualified intermediary. The intermediary could be made available by the system operator, but the person should be permitted to nominate his own intermediary provided he has suitable qualifications.

Given these precautions the data subject should not be prevented from inspecting or receiving a copy of the file.

(iii) Where the operation of the system would be seriously prejudiced by inspection of the information held about the person, and the importance of the system outweighs the privacy problem so generated.

This exception includes national security and criminal investigation files, and information collected in anticipation of court action.

Even in these situations, a method of achieving public knowledge is still necessary. Section 4 below contains the Committee's proposed method in such situations.

Guideline (7)(b) continued.

The following points are made concerning the procedure whereby data subjects are permitted access to their files:

(i) access should be acceptable by personal visit to the system operator's location, by post or by telephone. However, provided the arrangements are not unduly restrictive the system operator could establish an administrative procedure for handling applications;

(ii) the operator should take reasonable care in checking the identity of the person seeking access. Depending on the sensitivity of the data and its attractiveness to third parties, different types of identity checks may be appropriate, e.g.
- -check of signature;
- -production of suitable 'proof of identity' (e.g. driver's licence, bank pass book, credit card, birth certificate, organisation membership cards);
- -by mailing a copy to the person's address as recorded on the file (in some cases by registered mail);
- -fingerprints (only appropriate in the case of criminal law enforcement systems);

(iii) Where a suitable authority is provided, however, the system operator should deal with the data subject's nominee, on his behalf or in conjunction with him;

(iv) access should be permitted without any requirement that the data subject state a reason or in any way justify the need to gain access;

(v) the information should be provided in a form comprehensible to the recipient. For example where codes are used, either the information should be converted to its literal meaning, or an explanation should be supplied with it;

(vi) The committee would not think it unreasonable for a charge generally to be made for this service.

At this stage the Committee does not see the need to make non-compliance with the subject access guideline an offence (as has been done in Sweden, and in the U.S. for Federal Government Agencies).

Note also the comments about subject access made in guideline 3(d) above.

(c) Subject Knowledge of Accesses.

In most circumstances, the system operator should take reasonable steps to ensure that the subject knows when data about him is disseminated to a third party.

In particular this requires action in relation to:
- compulsory legal process, (e.g. subpoena and search warrant);
- other statutorily empowered demands, (e.g. by the Taxation Department under section 264 of the Income Tax Assessment Act, or by the Department of Social Security under Section 141 of the Social Services

Guideline (7) continued.

(d) Subject Complaint.

Where a data subject wishes to object to some feature of the system operator's handling of information about himself, then he should have some means open to him whereby he can have his complaint dealt with.

As expressed in Guideline (6)(c) in relation to more general matters, it is most important that organisations have mechanisms to receive complaints, to investigate them, and to communicate to the complainant the findings. This avoids small disputes unnecessarily becoming large ones, and reinforces public confidence in the organisations which service it.

Where the integrity of information held by the system is under dispute, the existence of the unsettled dispute should be recorded, and on any occasion the information is accessed internally, or disseminated, the fact that it is under dispute should also be communicated to the recipient.

Where the dispute relates to the completeness of the data, it may be appropriate to permit the data subject to append comments to the file. For example a person who has a default judgment recorded against him relating to an unpaid debt may wish to have recorded that he was unexpectedly hospitalised at the time.

(e) Subject Challenge and Enforcement.

Where a person is opposed to some feature of the operator's handling of certain data about himself, there should be an avenue available to him whereby he can seek to have the desired change enforced.

In very few situations does a ground presently exist whereby a member of the public can request the Courts to enforce deletion or correction. A complaint can be made to the Privacy Committee, which has the power to investigate and to make recommendations to the organisation concerned.

At some time in the future, with more experience of the extent to which such problems actually arise, the Committee may find it necessary to recommend the creation of some such ground. In the interim it is felt that the measures outlined below in Section 4 are adequate.

4. THE ROLE OF THE PRIVACY COMMITTEE.

A permanent privacy protection agency should exist on behalf of the public, to observe the impact of personal data systems on the privacy of individuals and to deal with complaints the parties have been unable to resolve.

The N.S.W. Privacy Committee is the agency charged with these responsibilities by the Government of N.S.W. It is a permanent body, created under Section 5(1) of the N.S.W. Privacy Committee Act, 1975. It comprises a representative group of people appointed according to a formula specified in Sections 5(3) and 5(4) of that Act.

The Committee performs the following functions in relation to the privacy impact of personal data systems:

- monitoring of the effectiveness of these guidelines;
- mediating in disputes;
- acting as an intermediary;
- researching into particular problems;
- educating the public on particular issues;
- accounting to the public.

(a) Monitoring of the Effectiveness of These Guidelines.

The Privacy Committee will actively seek public comment on the specific difficulties encountered in implementing these guidelines, and provide clarification as necessary, for a period of two years. It will advise system operators on appropriate methods of compliance with particular requirements, and will mediate between operators and persons or organisations who may differ in their opinions on certain aspects of systems. Through its complaints investigation function and information obtained from the public, it will be able to detect non-compliance with the guidelines. This will depend of course on the extent to which the public knows of it, and on the level of public concern as evidenced by letters to newspaper editors, to parliamentarians, media news items, etc.

The Committee feels that at this stage the cost of regular independent audit of the compliance by system operators with the guidelines, either by a government agency or by commercial auditors, is not warranted. Neither does it see any present need for registration or certification of data systems operators (as in Sweden, and probably soon in U.K.), nor for its approval to be given for new systems, mergers, or interconnections (as is also required in Sweden). It does, however, request system operators to raise such matters, especially interconnections, where the data is sensitive. Where it is apparent that more specific guidelines are required these will be prepared and distributed. This applies in particular to credit, criminal, medical and employment records and associated practices.

Where it is apparent that guidelines are not an effective solution, the Committee will recommend to the Government that specific legislation be enacted, perhaps involving penalties, the right of data subjects to compensation, registration etc.

(b) Mediating in Disputes.

The guidelines are intended to encourage operators to ensure they have a suitable degree of openness in their dealings with the public, and to enhance the public's confidence in organisations in both the public and private sectors. Hence it is anticipated that most disputes which arise will be capable of resolution by the parties themselves.

Section (4)(b) continued.

Where resolution is not possible, the Committee is authorised under Section 15(c) and (d) of its Act to investigate, to mediate between the parties and to recommend a solution. While the Committee is not an arbiter, in that it cannot enforce either party to accept its recommendation, it has very rarely had its decision ignored, and feels that at this stage enforcement powers would actually make it less effective. Its main success arises from the frankness and trust it receives from the parties, which would be hampered by the existence of enforcement powers.

(c) Acting as an Intermediary.

In some circumstances, it may be inappropriate for a data subject or an interested member of the public to deal directly with the data system operator. Examples are:

- where the volume of accesses or the detail requested, become prohibitively excessive, e.g. due to radical activism, or attempted exploitation for commercial gain (Guideline 6(b)(i));

- where the purpose of the system would be seriously prejudiced by inspection of the information held, e.g. national security and criminal intelligence files (Guidelines 6(b)(ii) and (7)(b)(iii));

- where the data may be in itself harmful to the subject, e.g. some psychiatric and medical records (Guideline (7)(b)(i));

- where the data is likely to be misinterpreted by the subject due to its technical content, with likely harmful effect, e.g. some psychiatric, psychological and medical records (Guideline (7)(b)(ii)).

In such circumstances the person should be able to brief an appropriate representative on his fears and on what he sees as the likely errors and injustices which may be contained in the file. In most circumstances he should be free to choose his own representative provided that person has appropriate qualifications.

On occasions the person may request the Privacy Committee to act as his intermediary.

In other circumstances, and in particular national security and criminal intelligence files, Parliament should nominate an intermediary, independent from the system operator, but bound by suitable secrecy provisions (this is the effect of provisions of the N.Z. Wanganui Computer Centre Act). A body similar to the Privacy Committee could be a suitable body to perform this function.

(d) Researching into Particular Problems.

The Privacy Committee conducts research into specific problems as and when necessary.

It is competent to do research of its own volition under Section 15(1)(a) and (g) of its Act, and under Section 16 has considerable powers as regards the collection of information. Recent or current studies have related to market research and public opinion surveys, identification techniques including photograph-bearing cards, law and practice relating to people's names, and publicly available lists of names and addresses.

Section 4 continued.

(e) Educating the Public on Particular Issues.

The Committee publicises the existence of particular problems, to inform the public, and so facilitate the democratic process. It is also able to dissipate unwarranted public fears.

It is competent to do this under Section 15(1)(f) of its Act. It frequently issues news releases, and is represented on radio and television, and at meetings, conferences etc.

(f) Accounting to the Public.

As the public's representative, the Committee is required to report publicly both annually and on particular matters as necessary.

It is required to report annually to the Minister (Section 17(1).), who is required to later report before Parliament as soon as practicable (Section 17(2)). The Committee, as a matter of policy, reports within three months of the conclusion of each calendar year.

Under Section 18 the Committee may also make special reports to the Minister on any matter at any time, and the Minister may make such a report public notwithstanding that it has not been presented to Parliament.

The Committee's powers of public statement (under Section 15(1)(f).) are also used to account to the public on particular matters.

5. GLOSSARY.

Access	(to information). Includes all types of communication of data maintained within a personal data system, to any person or organisation.
Accuracy	(of information). The close correspondence between the information recorded and the facts.
Archives	Data whose original purpose and uses have expired, but which has historical value, and is stored separately from 'live' data, and subject to additional security measures at least during the subject's life.
Completeness	(of information). The avoidance of using data without other data which is related to it in an important way.
Conditional Dissemination	(of information). Dissemination (q.v.) to an outside organisation on certain conditions relating to use, retention, dissemination, security etc.
Consent	(by a data subject). Permission given with a reasonable understanding of its implications, and without physical or psychological duress.
Corruption	(of data). The unjustified changing of data between the time it is collected and the time it is accessed.
Data	Used synonymously with Information.
Data Corruption	See Corruption.
Data Integrity	See Integrity.
Data Relevance	See Relevance.
Data Security	See Security.
Data Subject	The natural or legal person to whom the data relates.
Dissemination	(of information). Communication of data to a person outside the system operator's own organisation. (See also Access, Internal Access)
Identification	(of persons). The association of information with a particular natural or legal person.
Information	Used synonymously with Data.
Integrity	Fairness with which the information represents some factor about the person. This is influenced by the accuracy, the timeliness and the completeness of the information.
Interested Public	Those members of the public who have a demonstrable interest in the system, or who represent one or more members of the public who have a demonstrable interest. In particular this includes data subjects, and persons who may become data subjects.

Section 5 continued.

Internal Access	(to information). Communication of data to a person within the system operator's own organisation (See also Access, Dissemination.)
Law	Includes all forms of legal authority including legislation, regulation and approval by a body carrying Parliament's delegation.
Operator	See System Operator.
Person	Includes natural persons (humans) and legal persons (corporations, trusts, statutory bodies, etc.)
Personal Data	Particulars concerning any characteristic of an identifiable natural or legal person, or the affairs of that person.
Personal Data System	A collection of data files and procedures which collects, stores, processes and/or disseminates personal data.
Purpose	(of personal data system). The most abstract statement of objectives. See also Uses.
Relevance	(of data to a decision). The existence of a demonstrable relationship between the decision or determination being made, and the particular item of information.
Security	(of information). The precautions taken against unauthorised use and dissemination of information (note that the term is sometimes used to refer also to measures taken to ensure what is called in this paper "data integrity").
Sensitivity	(of information). The degree of importance which a given person places upon the non-disclosure of a given item of information.
Subject	See Data Subject.
System Operator	The person or organisation by whom or on whose behalf a personal data system (q.v.) is operated.
Timeliness	(of information). The earliness of updating of the file with new data.
Uses	(of personal data system). The set of operational objectives implied by the very general 'purpose' (q.v.)

6. APPENDIX: MORE DETAILED COMMENTS ON THE MAJOR DEFINITIONS.

(1) The Definitions.

Personal Data System: A collection of data files and procedures which collects, stores, processes and/or disseminates personal data.

File: A collection of similar records relating to different persons.

Record: A collection of items of information all of which relate to the same person.

Note that a record might be:

(a) several pieces of paper, clipped together or in a folder. (Sometimes this is referred to as a 'file'; this usage is avoided in this paper);

(b) a single piece of paper;

(c) part of a document which contains data about other persons as well.

Item: The most detailed level of meaningful information, e.g. first given name, year of birth, invoice number.

Personal Data: Particulars concerning any characteristic of an identifiable natural or legal person, or the affairs of the person.

(2) Specific Inclusions:

(a) Systems where the data cannot easily be accessed using the person's identity, e.g. cash receipts, journals, day books, where a searcher would need the receipt number or date to quickly locate the data.

Such files are, however, rarely likely to represent a serious privacy problem.

(b) Systems containing anonymous files in which the person is not directly identified, but where a cross-reference or index exists which enables the identification to be done. For example a debtor's file which only contains an account number is anonymous, but still represents a potential privacy problem since a listing of debtor's numbers and names exists.

(3) Specific Exclusions.

(a) Uncirculated personal notes, papers and records which are retained or discarded at the author's discretion, and over which the system operator has no control, e.g. personal telephone lists and notes on blotters;

(b) Personal memory;

(c) Statistical systems, i.e. systems in which the person is not identifiable since:

(i) no identifying particulars are stored (i.e. no name or account number etc.); and

Section (6)(3)(c) continued.

(ii) the descriptive data kept is not sufficiently detailed to enable identification by correlation (e.g. a file which contains home address, age and sex is identifiable, not statistical).

(4) The System Operator.

By this is meant the person or organisation by whom or on whose behalf a personal data system is operated.

It is therefore not merely the record-keeper or data-processor (which may be a specialist section of the organisation, or even an external agency such as a computer service bureau). It is the department, section, company or other entity which is the main user of the information that must take the prime responsibility for the system. In computer jargon this is commonly called the 'user' or 'user department'.

Clearly some portions of these Guidelines will be of more direct relevance to the specialists or sub-contractors who actually perform the collection and maintenance of the information. The responsibility for ensuring the Guidelines are observed is that of the person for whom those specialists or sub-contractors are performing the work.

(5) Internal Access Versus External Dissemination.

Internal access to information is communication to persons within the system operator's own organisation; any other communication is an external dissemination.

At times there will be uncertainty as to the boundary between internal and external, e.g. different divisions of the same company, companies in the same group, or sections in the same government agency.

Where such uncertainty exists the problem is best resolved by referring to the general purpose and specific uses of the system. Where these clearly involve both parts of the organisation then it is an internal access (e.g. both sales and accounts sections need access to the name and address of credit account customers). But where a part of an organisation is not clearly involved in the purpose, then it is an external dissemination (e.g. the customer list of a building products subsidiary is not in the normal course accessible by another subsidiary dealing in say consumer appliances).