Journal and Proceedings of The Royal Society of New South Wales

Volume 115 Parts 3 and 4 [*Issued February, 1983*]

pp.91-94 Return to CONTENTS

Privacy and Modern Science and Technology

W.J. Orme

[Text of an Address presented to the Symposium on "Ethical Problems of Modern Science and Technology, conducted by the Royal Society of New South Wales, 4th November, 1981]

1. Balancing Privacy and Fundamental Freedoms and Public Interest

1.1 Generally

One of the main reasons which makes privacy so complex is that it is not a separate entity which can be defined and evaluated in isolation, but is a factor in most aspects of modern life and, on some occasions. must give way to more important social objectives.

1.2 Privacy and Research

Privacy only becomes an issue when identifiable personal information is used. Equally, surveys and questions on a totally voluntary and unidentifiable basis do not create privacy problems.

Many researchers come to the Committee to discuss their questions and methodology in advance. The Committee's accumulated experience can be of assistance in the planning stages. Avoiding pitfalls can increase both response rate and the quality of the information.

The Committee does not evaluate the objectives of the research. Our function is to assist the researcher to achieve the desired objective without unjustified invasions of privacy. The Committee would wish to avoid the creation of licensing or government permission as a pre-requisite to conducting research. This would be a major fetter on scientific freedom.

1.3 Absolute Freedom of Research?

While privacy is not an absolute right neither is there an absolute right of a researcher to invade privacy within the armour of academic freedom.

Each must find an effective working relationship with the other, The scientist who can not see how an individual's privacy is affected by a research project, which to him is one of vital importance, does science a disservice.

Particularly, I note that some researchers who argue so vehemently for their own research to be unfettered by privacy, are the first to complain when their own privacy is invaded by another.

2. Ingenuity Avoids Conflicts

We have found that, with reasonable care and ingenuity, most research objectives can be fairly achieved. One might even ask, who should have greater ingenuity than a competent researcher?

For example, the Committee was approached after researchers had been refused access to medical insurance fund data on women who had had hysterectomies. They wished to contact the women but the fund quite properly refused to supply the names and addresses.

While agreeing with the fund, the Committee recommended that it should send an explanation of the survey to the women on behalf of the research body. The explanation would outline the purpose of the research and ask those women who wished to participate to contact the researchers direct. This method was adopted and more than sufficient women volunteered to participate in the survey.

Many other examples are set out in the Committee's annual reports.

Researchers are invited to contact the Committee to discuss their proposals or problems that might arise during the course of research, at any time. (Copies of the Committee's two relevant papers on the subject, Guidelines for Surveys – No. 42, November,1979, Research and Confidential Data: Guidelines for Access – No. 35 September, 1978 are available from the Committee on request.

3. What Confidentiality can a Researcher Promise?

The Committee finds that confidentiality can be breached as a result of subpoenas, government powers, search warrants etc., professional clumsiness or lack of physical security. These should all be borne in mind when confidentiality is promised.

3.1 Subpoenas, Government Powers and Search Warrants

There are many provisions for subpoenas, search warrants and other Government powers which make absolute confidentiality impossible. The Committee has developed guidelines with judges, police and other relevant bodies which have worked successfully in New South Wales since they were published in July, 1980. They are too complex to deal with in the time available but they have been widely circulated through professional bodies and magazines and copies are available from the Committee on request (see Appendix).

I might say, however, that the Committee is currently questioning some of the Government powers that do exist and will be reporting on its concern soon.

3.2 Professional Clumsiness

Sheer clumsiness can cause substantial embarrassment to research subjects. A doctor's patient complained to the Committee that he had identified her without her consent, in a case study submitted by him as part of his application for membership of a professional college. The conduct of both the doctor and the College confirmed this view even though they vehemently denied the allegation.

With the consent of the woman I inspected the case study and found that not only did the anonymised details clearly identify the woman but also the woman's actual name and address was clearly typed on the front page. The College was highly embarrassed by the lack of professionalism and the case study was promptly destroyed by way of apology.

3.3 Physical Security

It is dangerous to rely on physical security. Inadvertent breaches of security and accesses by investigators for proper and improper purposes by improper methods will inevitably occur. The main lesson is, "don't become over confident and thereby complacent."

I recently offered a leading hospital who appeared to me to be over-confident about their security a ten-to-one bet that I could obtain, with his consent, the file of my nephew held by a leading hospital within twenty four hours. The hospital did not take the bet but I checked with the investigator I would have used, to ask if he could have won the bet for me. He asked if I were prepared to pay for special delivery, in which case he could have got the file for me within two hours. This is a fact of life.

4. The Examples of Problems Encountered by the Committee Arising from Research Registers

(i) Central Indexes

The Committee is concerned that some hospitals transfer identified patient data to central registries without the patient's consent. Also judgements are called for which can be prejudicial to the patient (for instance assessing his attitude to work). The Committee believes that, wherever possible, if not at all times, information reported to such indexes without the patient's full and informed consent should be in an anonymised form with the capacity to go back through the hospital to the patient where normal ethical controls will apply.

(ii) Genetic Defect Registers

Again, no matter how desirable these might be, informed consent is highly desirable, if not essential. Any exceptions to the consent rule should be established by specific legislation following public debate.

(iii) Attitude of Parents

One hospital planned to ask obstetric sisters to record, on the birth records, their view as to whether or not they thought the mother really wanted the child at the time of the birth. No doubt there was a real research interest in correlating that information with subsequent conduct such as child abuse. However, it was a highly objectionable and dangerous proposal which was quickly dropped.

(iv) Drug and Alcohol Registries

A listing of all drinking habits in a central register was also discontinued after discussion with the Committee.

You must bear in mind that all this information can be subpoenaed in subsequent family law disputes or be subject to search warrant, Consumer Affairs accesses etc.

5. Conclusion

Commonsense and ingenuity can ensure that scientific and technological research objectives can be achieved, and at the same time the researchers can maintain the respect of the public who are the subject of the research and who are presumably served by it.

APPENDIX

SUBPOENA OF SENSITIVE RECORDS:

PROCEDURES FOR PROTECTING PRIVACY
(including search warrants and other official demands)

1. INTRODUCTION

From time to time the Privacy Committee receives complaints that sensitive personal data is produced in court pursuant to a subpoena, or is accessed as a result of a search warrant or other official demand, either without the subject's knowledge or in a way which the data keeper thinks unjustifiably invades his privacy.

While medical and bank records are the more usual type of records which give rise to the problem, it can apply to almost any record, such as:

(a) Education – pubils' school reports and cards; counselling reports.
(b) Employment personal files held on employees.
(c) Insurance policies; reports prepared on claimants.
(d) Finance – credit transactions; wages and income records; home loans; real estate transactions; taxation returns.
(e) Social Work – counselling reports; individual assessments and references.
(f) Adoption – reports maintained by the Department of Youth & Community Services.
(g) Libraries – borrowing patterns and preferences.

What is Sensitive Data?: The prime criterion of sensitivity is whether the data subject considers data sensitive. Wherever a data keeper receives a subpoena dealing with someone else's data, he should immediately advise the data subject of the fact that the subpoena has been received and wherever possible take his views into account and include them in a covering letter as suggested.

2. TYPES OF PROBLEM

2.1 Medical Records:

Three examples are:

(a) Where the Patient's Medical Record contains Information on Other Persons

This is most likely to arise in respect of families. It is not uncommon for doctors to open a file on a patient and to include references to his spouse and children in the same file. This has obvious advantages in relation to familial and communicable illnesses.

(b) Where the Patient's Medical Record contains Sensitive Personal Information

A clear example of this would be in a negligence action for damages where a woman is claiming damages for an iniury to her arm. It would generally be irrelevant to the proceedings to know that she had a termination of pregnancy some three years prior to the accident.

(c) Where the Doctor Considers it would be harmful to the Patient to know of his Medical Condition

It is likely that such cases would only arise on rare occasions, e.g. where the patient is suffering from a serious illness and could, if told, attempt to commit suicide.

2.2 Bank Records:

Three examples are:

(a) Where the Subject's Record contains sensitive Information irrelevant to the Proceedings

An example of this could arise in proceedings for settling a property dispute where information not related to that dispute is also included in the record.

(b) Where the Subject's Bank Record contains Information on other Persons

This is likely to arise in respect of families, partnerships, etc. where the financial dealings of a person who is not a party to the proceedings, or involved in them in any way, are mentioned in the subject's record.

(c) Where the Record of a Person who is not a Party to the Proceedings is subpoenaed and it (or any part of it) is not relevant to the Proceedings

X, who was to be married to Y, had her financial records subpoenaed by Y's former wife in connection with a property dispute arising out of the dissolution of a former marriage.

X was required to produce her taxation returns, cheque butts, bank statements, insurance policies, documents relating to the purchase of real estate, wages and income records etc.; her bank was also subpoenaed to produce records of her account. X alleged that these records were irrelevant to the proceedings and that it amounted to an invasion of her privacy, particularly as she was an independent person who did not wish her prospective husband to know the full details of her financial affairs.

3. RECOMMENDATIONS TO DATA KEEPERS WHEN RECEIVING A SUBPOENA

3.1 Subpoenas

Judges will take privacy factors into account if the factors are drawn to their attention. Whenever a data keeper receives a subpoena which raises a privacy issue he should –

(a) forward the record to the court in a sealed envelope marked "Judge Only.

(b) send a covering letter to the Judge setting out his concern for the data subject, and his reasons for such concern if the particular records are produced in open court;

(c) *advise the data subject of the subpoena so that the data subject may either be represented by a solicitor or appear in person at the court and ask the Judge to be heard on reasons why his file should not be tendered in open court.*

This will enable the Judge to:

(a) *discuss the relevance to the case and the privacy issues with the legal representatives (or, where appropriate, the person) before opening the envelope, to ensure that access to the record is necessary;*

(b) *if access is insisted upon, inspect the record himself to ensure that only relevant informtion is produced in court.*

The above procedures will enable Judges, having regard to the requirements of justice and other competing interests, to ensure that privacy is protected as far as possible.

It should be clear that if the party subpoenaing the records can show that they are relevant, and insists that they be produced in open court, this will in fact occur.

3.2 Search Warrants and Powers of Demand and Search

i Notification to the Data Subject

Wherever an official demand for access to data occurs, the data subject should be advised as provided for in the recommended procedure (para. 3.1 above). In some instances it is not in the public interest that the data subject be notified while police investigations are taking place. It could be appropriate to advise the Committee of any requests not to notify, for advice and for the Committee's research purposes.

ii Questioning an Official Demand

In some instances the official demand, such as a search warrant or use of a power under a particular statute, might create an invasion of privacy which is not justified by the public benefit that flows from it. If the data keeper is in any doubt the Committee should be contacted for advice and assistance, The Committee's experience is that responsible decisions are almost always taken by public sector bodies where the appropriate facts and consequences are brought to their attention.

iii Confidentiality of Mass Health Care Records during Police Investigations

Guidelines have been arrived at between the N.S.W. Police Department, the Privacy Committee, and the Law Society, Bar Association and Australian Medical Association (N.S.W. Branch) to protect privacy when such investigations occur. A copy of the guidelines is attached.

4. ASSISTANCE FROM THE PRIVACY COMMITTEE

Introduced with goodwill and commonsense it is hoped that the unusual types of problems that have come to the Committee's attention will be avoided. Where the above procedures do not provide an adequate protection, either the data keeper or the data subject should approach the Committee for advice and, if necessary, assistance.

In general, the Privacy Committee will not be able to interfere in any way with matters before the court. However, by providing a centre of research and experience in this area it is hoped that if the problems are not solved a more effective remedy will be devised.

MEDICAL
CONFIDENTIALITY OF PROFESSIONAL RECORDS
DURING POLICE INVESTIGATIONS
GUIDELINES

1. A panel of medical practitioners should be formed to assist Police in the interpretation of medical records.
2. Any mass seizure by warrant of medical records should be carried out only under the supervision of experienced investigators.
3. If practicable, the assistance of a member of the panel should be sought and he should be requested to be in attendance at the seizure.
4. If practicable, records (the subject of the warrant) should be inspected at the premises being searched and only those records considered relevant to the investigation should be seized.
5. A descriptive list should be made and kept of records which are seized.
6. If the medical practitioner concerned indicates that he needs the records seized to enable him to continue the treatment of the patients, he should be supplied with photocopies as soon as practicable.
7. All records which have been seized should be kept in a place of security and only persons involved in the investigation should have access to them.
8. In the event of a patient seeking particulars of the seizure of his medical records, he should be advised to make such request through the office of the Commissioner of Police.

These guidelines would also be applicable where other types of confidential professional records (e.g. solicitors' or accountants, records) were sought for police investigations.

Return to Top