

*P. Hamilton*  
*25/6/92*  
*Please return*

---

**Data-matching Program**

**SELECTED EXTRACTS FROM THE  
PROGRAM PROTOCOL  
DATA-MATCHING PROGRAM  
(ASSISTANCE AND TAX)**

---

**Prepared by the Department of Social Security pursuant to  
Guideline 3 of the Schedule to the Data-matching Program  
(Assistance and Tax) Act 1990.**

SECTION 10 TIME LIMITS ON CONDUCT OF PROGRAM

---

Section 21 of the Data-matching Program (Assistance and Tax) Act 1990 specifies that Parts 1 and 2 of the Act will cease to be in force at the expiration of 2 years after the date of commencement of the Act. This is a 'sunset clause' and means that the Data-matching Program cannot continue for more than two years unless new legislation is passed by the Parliament which extends the life-span of the initiative.

---

SELECTED EXTRACTS FROM THE  
PROGRAM PROTOCOL  
DATA-MATCHING PROGRAM  
(ASSISTANCE AND TAX)

Prepared by the Department of Social Security pursuant to Guideline 3 of the Schedule to the Data-matching Program (Assistance and Tax) Act 1990.

**Note:** The full program protocol has more than 100 pages and includes the text of all the relevant legislation. This paper includes only certain sections - indicated on the contents page overleaf, which are judged to be of particular interest to members of the public.

The full protocol, or any other sections, are available free of charge from

The Privacy Commissioner  
Human Rights and Equal Opportunity Commission  
GPO Box 5218  
SYDNEY NSW 2001

Toll free from anywhere in Australia: 008 023 985



## CONTENTS

* PRELIMINARY MATTERS	
* SECTION 1	MATCHING AGENCY AND SOURCE AGENCIES
SECTION 2	LEGAL BASES FOR ANY COLLECTION USE OR DISCLOSURE OF INFORMATION INVOLVED IN THE PROGRAM
* SECTION 3	OBJECTIVES OF THE PROGRAM AND RELATED MATTERS
	(a) Objectives of and Justification for the Program
	(b) Procedures to be employed
	(c) Nature and Frequency of Matching
* SECTION 4	ALTERNATIVE METHODS
* SECTION 5	COST/BENEFIT ANALYSIS
SECTION 6	OUTLINE OF TECHNICAL CONTROLS
* SECTION 7	USE OF IDENTIFICATION NUMBERS
* SECTION 8	OUTLINE OF ACTION ARISING FROM DATA-MATCHING
* SECTION 9	NOTICES TO INDIVIDUALS ABOUT EXISTENCE OF THE DATA-MATCHING PROGRAM
* SECTION 10	TIME-LIMITS ON CONDUCT OF THE PROGRAM
APPENDIX 1	DATA-MATCHING PROGRAM (ASSISTANCE AND TAX) ACT 1990
APPENDIX 2	OTHER LEGISLATION
APPENDIX 3	FORMS AND LETTERS

## SECTION 9 NOTICES TO INDIVIDUALS ABOUT EXISTENCE OF DATA-MATCHING PROGRAM

The Schedule to the Data-matching Program (Assistance and Tax) Act 1990 requires that Source Agencies inform their clients in writing of the fact that the information they have supplied to the Source Agencies may be used in data-matching. The notice may be given either before information is first used in data-matching or as soon as practicable after the information is used.

Each Source Agency will determine how it will satisfy this requirement.

In the case of the Tax Agency, agreement has been reached that other Source Agencies when writing to their clients will mention that information the clients have provided to the Australian Taxation Office may also be used in data-matching.

In the interests of keeping the costs of satisfying the requirement to acceptable levels, it is likely that most Source Agencies will make use of scheduled mailouts to clients and include advice about data-matching with the other correspondence being sent to their clients. Some special mailings may be necessary for clients who are not scheduled to receive other correspondence within a reasonable timeframe.

Where scheduled mailouts will not occur for some months, media publicity may also be used as a way to convey information about the data-matching program to clients quickly.

\* These Sections are included in this paper.



Similar provisions apply to the Tax Agency in respect of its clients.

Source Agencies are developing proformas of the letters they will be using to approach clients about whom they have been informed of a discrepancy. As those letters are developed and cleared they will be provided as an appendix to the Program Protocol.

---

## PRELIMINARY MATTERS

---

'Data-matching' is the comparison of two or more sets of data to identify similarities or dissimilarities. In the context of this Protocol, the term is used to denote the use of computer techniques to compare data found in two or more computer files to identify cases where there is risk of incorrect payment of personal financial assistance or of tax evasion.

The 'Data-matching Program' is the system of data-matching as defined in Section 6 of the Data-matching Program (Assistance and Tax) Act 1990.

A copy of the Data-matching Program (Assistance and Tax) Act 1990 may be found at Appendix 1.

## BACKGROUND

The Department of Social Security began using computer data-matching of client information in 1979 to verify identity, income and other aspects of eligibility for income-support payments. Other Agencies have also applied this approach with the aim of identifying clients who may have misrepresented their circumstances and who may be ineligible for the assistance they are receiving or may be receiving assistance at an incorrect rate.

Data given to the Department by other Agencies (State or Commonwealth) is provided in accordance with legal requirements. Most of the projects for which data has been sought have been announced publicly as part of the Government's Economic Statements or Budgets. This has invariably been the case in recent years.

The secrecy provisions of the Social Security Act 1947 apply to information obtained from other Agencies, just as they do to Social Security client data. These provisions are discussed in detail in Section 2 of this document.

## RECENT DEVELOPMENTS

In the 1990/91 Budget the Government announced new measures to detect incorrect payments in the income-support system. These involve:

- the use of Tax File Numbers to assist in the automatic verification with the Australian Taxation Office of income information supplied by clients seeking Government income-support payments (this information is currently checked manually), and
- increased use of data-matching between various Government Agencies making financial assistance payments, especially the Departments of:



- Social Security;
- Employment, Education and Training;
- Veterans' Affairs, and
- Community Services and Health (First Home Owners Scheme only)

to detect "double payments" - ie. instances in which people collect more than one payment, usually from different Agencies, where no entitlement exists to one or more of the payments.

The rationale for the new measures adopted by the Government is that further major savings in financial assistance payments can be made if ADP technology is employed which facilitates the automatic checking of data across Agencies.

These savings cannot be achieved using labour intensive, manual checking techniques.

#### IMPLEMENTATION OF THE NEW MEASURES

The decision announced in the 1990/91 Budget to extend the requirement to provide Tax File Numbers and the subsequent matching of data is embodied in four pieces of legislation:

- . Social Security and Veterans' Affairs Legislation Amendment Act (No. 2) 1990;
- . Social Security Legislation Amendment Act 1990;
- . Student Assistance Amendment Bill 1991, and
- . Data-matching Program (Assistance and Tax) Act 1990.

The Social Security and Veterans' Affairs Legislation Amendment Act (No. 2) 1990 and the Social Security Legislation Amendment Act 1990 received Royal Assent on 28 December 1990 and 8 January 1991 respectively. They extend the requirement to provide a Tax File Number, which previously applied to certain Social Security and Department of Employment, Education and Training clients, to virtually all clients receiving personal financial assistance payments under the:

- . Social Security Act 1947;
- . Veterans' Entitlements Act 1986;
- . Seamen's War Pensions and Allowances Act 1940; and
- . First Home Owners Scheme.

The Student Assistance Amendment Bill 1991, currently before Parliament, proposes similar extensions of Tax File Number requirements in respect of payments under the Student Assistance Act 1973 (Austudy and Abstudy).

#### SECTION 8 OUTLINE OF ACTION ARISING FROM DATA-MATCHING

In the longer term when data-matching routines have been thoroughly tested and proven, the information provided by the Data-Matching Agency to Source Agencies may, in many cases, be used to produce automatically generated letters to the clients in respect of whom discrepancies have been identified. However, there will be some instances where this cannot be done because it will never be possible to reach a level of confidence with all matches that will allow the generation of automatic letters in respect of all discrepant cases.

Source Agencies will take a conservative approach and subject discrepancy reports to some form of preliminary investigation before deciding to approach clients. The need for this will reduce over time as experience is gained about discrepant cases. In the case of clear cut discrepancies eg. incontrovertible evidence of the receipt of inconsistent payments, it would be possible to make a prompt approach to the client. For other cases eg. where there are apparent income discrepancies, a more comprehensive preliminary investigation would probably be warranted.

It will be the responsibility of Source Agencies to make arrangements for the assessment and follow-up of discrepancies advised to them. Agencies with a decentralised structure may choose to have most follow-up action taken in Areas or Regions. Less decentralised Agencies may choose to concentrate follow-up action in Central or State Offices.

Whatever approach Agencies take towards follow-up action, Section 10 of the Data-matching Program (Assistance and Tax) Act 1990 requires that Agencies must make a decision to take action or to carry out an investigation of the need to take action within 90 days of the receipt of notice of discrepancies or they must destroy the information received.

Section 11 of the Data-matching Program (Assistance and Tax) Act 1990 requires that Assistance Agencies not take action to suspend, cancel, reject or reduce the rate of personal assistance or to recover an existing overpayment unless they have first written to the client concerned. That letter must give the client particulars of the information which has been obtained through data-matching and identify the action it is proposed to take. Furthermore, the letter must give the client 21 days from receipt of the letter in which to show cause in writing why any proposed action should not be taken. (The client need not be informed if doing so would prejudice the effectiveness of an investigation into the possible commission of an offence.)



## SECTION 7 USE OF IDENTIFICATION NUMBERS

---

Section 7 of the Data-matching Program (Assistance and Tax) Act 1990 clearly defines the use of identification numbers, including Tax File Numbers, in the various steps of a matching cycle.

The first step of the matching cycle specifies that Assistance Agencies supply to the Data-Matching Agency basic data about their clients. This information will include the client's Tax File Number and the client's unique Assistance Agency identification number.

The unique Assistance Agency identification numbers are important because they are the means by which Agencies identify client records. They can be likened to a key to a particular client record. Both the key and the record are unique, so information about one client cannot be confused with information about another. Such confusion could easily occur if client records were identified by name only. Government Agencies deal with very large numbers of clients and the incidence of common or very similar names is high. The use of unique identification numbers gives Agency records an integrity they would otherwise lack and protects the privacy of clients by guarding against the mistaken use of information they provide to Agencies.

Provision of the Assistance Agency identification number to the Data-Matching Agency will help ensure that information about different clients is not confused during the various matching routines to be performed. It will also allow the Data-Matching Agency to clearly identify clients when returning information on discrepancies to the Assistance Agencies. Tax File Numbers will not be used for that purpose.

Tax File Numbers are the unique identifiers used by the Australian Taxation Office to identify taxpayers. As part of the proposed matching process, the Australian Taxation Office is to extract specified data from its records and to provide that data to the Data-Matching Agency. It is important that these extraction processes be as accurate as possible to protect the integrity of subsequent steps in the matching process. Matching with tax records could not be nearly as precise without the use of Tax File Numbers. This is the key reason they will be used in the matching process.

The only subsidiary and relatively minor use proposed for the Tax File Numbers is as a 'tie-breaker' in the event that the identity matching in step 4 of a matching cycle produces cases which cannot otherwise be separated.

Where specified in the legislation, Tax File Numbers must be provided in respect of spouses and parents as their incomes may have a bearing on the eligibility of a client to a particular payment or on the level of payment he or she is entitled to receive.

The Data-matching Program (Assistance and Tax) Act 1990 which received Royal Assent on 23 January 1991 provides the authority for the matching by a Data-Matching Agency of certain data held by the Australian Taxation Office and by the Departments of Social Security, Employment, Education and Training, Veterans' Affairs and Community Services and Health (First Home Owners Scheme only).

The Schedule to the Data-matching Program (Assistance and Tax) Act 1990 requires that a Program Protocol be prepared by the Data-Matching Agency in consultation with the Source Agencies. The purpose of this document is to:

- . identify the Matching Agency and the Source Agencies;
- . in the case of each Agency involved in the Program, set out the legal basis for any collection, use or disclosure of personal information involved in the Program;
- . outline the objectives of the Program, the procedures to be employed, the nature and frequency of the matching covered by the Program and the justifications for it;
- . explain what methods other than data-matching were available and why they were rejected;
- . detail any cost/benefit analysis or other measures of effectiveness which were taken into account in deciding to initiate the Program;
- . outline the technical controls proposed to ensure data quality, integrity and security in the conduct of the Program;
- . provide an explanation for any use of identification numbers and, in particular, tax file numbers;
- . outline the nature of the action proposed to be taken in relation to the results of the Program including the pro-formas of any letters to be used by Source Agencies when providing notice under section 11 of the Act;
- . indicate what form of notice, if any, of the proposed activities in relation to their personal information has been given or is intended to be given to affected individuals, and
- . specify any time limits on the conduct of the Program.



Agencies involved in data-matching undertaken under the authority of the Data-matching Program (Assistance and Tax) Act 1990 must observe privacy principles. People who consider that an Agency has interfered with their privacy by a breach of Part 2 of the Act, which sets out provisions for data-matching, use of the results of the data-matching program and includes provisions relating to privacy and confidentiality, may complain to the Privacy Commissioner.

---

Family Allowance

- Estimated population	1,900,000 cases	
- Estimated residual incorrect payment rate	2 per cent	
- Estimated cancellations	38,000 cases	
- Estimated \$ savings per case per fin yr		
- Estimated Gross Savings in a full fin yr	800	\$ 30.4m
TOTAL ESTIMATED GROSS SAVINGS IN A FULL FINANCIAL YEAR FROM DATA-MATCHING DECISION		<u>\$291.3</u>



#### Job Search Allowance

- Estimated population	14,300 cases	
- Estimated residual incorrect payment rate	2 per cent	
- Estimated cancellations	286 cases	
- Estimated \$ savings per case per fin yr	2,650	
- Estimated Gross Savings in a full fin yr		\$ 0.8m

#### Sole Parent Pension

- Estimated population	249,200 cases	
- Estimated residual incorrect payment rate	2 per cent	
- Estimated cancellations	4,984 cases	
- Estimated \$ savings per case per fin yr	6,500	
- Estimated Gross Savings in a full fin yr		\$ 32.4m

#### Age & Invalid Pension (Cancellations)

- Estimated population	1,723,000 cases	
- Estimated residual incorrect payment rate leading to cancellation	1 per cent	
- Estimated cancellations	17,230 cases	
- Estimated \$ savings per case per fin yr	7,250	
- Estimated Gross Savings in a full fin yr		\$124.9m

#### Age & Invalid Pension (Reductions in fortnightly payment)

- Estimated population	1,723,000 cases	
- Estimated residual incorrect payment rate leading to reduction in fortnightly payment	2.5 per cent	
- Estimated reductions	43,075 cases	
- Estimated \$ savings per case per fin yr	780	
- Estimated Gross Savings in a full fin yr		\$ 33.6m

#### SECTION 1: MATCHING AGENCY AND SOURCE AGENCIES

Section 4 of the Data-matching Program (Assistance and Tax) Act 1990 (the Act) provides for the establishment of a Matching Agency to match data supplied to it by Source Agencies.

A copy of the Data-matching Program (Assistance and Tax) Act 1990 may be found at Appendix 1.

#### MATCHING AGENCY

The 'Matching Agency' will comprise officers of the Department of Social Security who are responsible for the matching of data under the Act. They will be nominated by the Secretary of the Department and designated as the Data-Matching Agency.

Officers working in the Data-Matching Agency will be responsible for:

- . receiving data from Source Agencies;
- . matching the data;
- . ensuring the security of data during processing;
- . returning information to Source Agencies on discrepant cases identified through the matching process, and
- . the destruction of data at the end of the matching process.

While operating as part of the Data-Matching Agency, these officers will not have access to Social Security client information other than that provided to the Data-Matching Agency by the Department of Social Security in its capacity as a Source Agency. The confidentiality and security provisions which will apply to Data-Matching Agency operations are discussed further in Sections 3 and 8 of this document.

#### SOURCE AGENCIES

Source Agencies are those Commonwealth Government Agencies which will supply data to the Data-Matching Agency for the purposes of data-matching.

Source Agencies comprise the Australian Taxation Office (Tax Agency) and Assistance Agencies.

#### ASSISTANCE AGENCIES

The Assistance Agencies are the:

- . Department of Social Security (DSS);
- . Department of Employment, Education and Training (DEET);
- . Department of Veterans' Affairs (DVA), and the
- . Department of Community Services and Health (DCS&H).



### SECTION 3 OBJECTIVES OF THE PROGRAM AND RELATED MATTERS

This section outlines what the Data-matching Program is designed to achieve and explains why these measures are a vital addition to incorrect payment detection work already carried out by income-support Agencies.

#### OBJECTIVES OF AND JUSTIFICATION FOR THE PROGRAM

The overall objective of the Data-matching Program is to:

- . verify, independently and automatically, the accuracy of information disclosed to Agencies which make income-support payments, and
- . detect instances where persons could be receiving incorrect payments from an income-support Agency.

The purpose of the data-matching is to identify the following:

- . 'double payments' ie. instances in which people collect more than one payment, usually from different Agencies, where no entitlement exists to one or more of the payments;
- . non-disclosure of correct income for the purposes of obtaining or continuing to receive an income-support payment or an incorrect level of payment;
- . fictitious or assumed identities used by individuals to obtain payments to which they are not entitled;
- . tax evasion;
- . opportunities for re-raising overpayments of Government income-support so they can be recovered;
- . incorrect declaration of the number of dependants, and
- . inconsistent domestic circumstances cases (i.e. a client who is claiming as a single entity although he or she is living in a married or de facto relationship).

The achievement of these objectives will enable significant savings to be made and the redistribution of public revenue to areas of most need.

Public knowledge of the Data-matching Program will result in increased compliance with the eligibility requirements for personal assistance and the requirements of the taxation system.

### Financial Benefits

When the Government decided in the 1990/91 Budget, to proceed with data-matching arrangements, it took into account that there was a Social Security income-support population of over 4 million people with average annual individual amounts of payment ranging from around \$800 for Family Allowees to \$7,900 for Special Benefit. There was a belief that a randomly distributed incorrect payment rate of around 2 per cent existed throughout that population.

The following calculations were based on those parameters. (The actual numbers of recipients are now higher in most cases):

#### Unemployment Benefit

- Estimated population	373,600 cases
- Estimated residual incorrect payment rate	2 per cent
- Estimated cancellations	7,472 cases
- Estimated \$ savings per case per fin yr	7,280
- Estimated Gross Savings in a full fin yr	\$ 54.4m

#### Sickness-Benefit

- Estimated population	78,800 cases
- Estimated residual incorrect payment rate	2 per cent
- Estimated cancellations	1,576 cases
- Estimated \$ savings per case per fin year	6,980
- Estimated Gross Savings in a full fin yr	\$ 11.0m

#### Special Benefit

- Estimated population	24,300 cases
- Estimated residual incorrect payment rate	2 per cent
- Estimated cancellations	486 cases
- Estimated \$ savings per case per fin yr	7,900
- Estimated Gross Savings in a full fin yr	\$ 3.8m



Within the Social Security portfolio other net costs identified were \$1.25m for publicity associated with changes in the requirements for clients to provide Tax File Numbers, \$2m as a share of Australian Taxation Office costs associated with collection of Tax File Numbers and \$100,000 supplementation for the Privacy Commissioner's Office so suitably qualified staff could be recruited. It was estimated that other implementation costs would be offset by savings made available through the new matching program. Three major areas of saving were identified: staff savings flowing from the reduction in client populations as clients voluntarily surrendered payments or had their payments cancelled, savings in postage as the new matching program removed the need for a substantial portion of current mail reviews of clients' circumstances and savings in clerical effort associated with some reviews which would no longer need to be done after the introduction of the new matching arrangements.

The identified costs taken into account for the Australian Taxation Office were \$4.5m and were shared by DSS as mentioned above.

Identified costs for the Department of Veterans' Affairs were \$0.9m in running costs in 1990/91 and 1991/92 and \$0.1m in 1992/93 and 1993/94.

The estimated savings in program expenditure far exceed implementation and on-going costs.

#### Social Considerations

There are two key social issues associated with the initiative. One is the desire of most taxpayers for the welfare system to be secure from cheating and fraud. The other is the concern to protect the individual right to privacy.

Allied to the concerns most people have to see a welfare system with a high degree of financial integrity is a concern for social justice. In particular, there is strong support in the community for a welfare system which directs available funds to those most in need of assistance. The new measures help to achieve that in several ways. First, by strengthening controls in financial assistance payment systems it will significantly reduce the leakage of funds from those systems. This provides funds for Government to direct to other priorities. Second, the existence of effective controls in payment systems soon becomes evident to the community and rapidly increases voluntary compliance. When people realise that there is a high probability of incorrect payments being detected they are much more likely to meet their obligations under the law.

Suitable safeguards against unreasonable intrusion into people's privacy are being built into the data-matching arrangements. To this end, in addition to normal safeguards, the Privacy Commissioner is being consulted about the arrangements as implementation proceeds. He will monitor implementation of the initiative and will continue to be consulted on all major aspects of it.

#### Existing Control Measures

The Assistance Agencies involved in the Data-matching Program use procedures designed to prevent the incidence of incorrect payment. Clients are required, for example, to provide documentary evidence to support proof of identity, cessation of employment, evidence of income, or studies.

This information may be verified with employers, financial or educational institutions and Commonwealth Agencies such as the Australian Taxation Office. The reference data which is obtained from the Australian Electoral Commission and the Health Insurance Commission, may also be used to help verify identity.

Each Agency undertakes some internal checking of the information supplied by clients with existing records to ensure that duplication of payment does not occur.

Various measures are used by Assistance Agencies to review clients' entitlements.

#### Department of Social Security

There have been significant improvements in the integrity of the social security system through administrative reforms. These include heavy emphasis on the control of incorrect payment and fraud. Detailed results of current control measures are set out in the Department's Annual Report.

The Department concentrates on those cases where there is believed to be a higher than average risk of incorrect payment. This approach ensures that more wrong payments are detected and corrected than otherwise would be the case with any given level of resources.

It also emphasises to persons receiving income-support payments, that non-compliance, whether deliberate or not, is likely to be detected and that there are penalties including repayment of the money owing and, in some cases, prosecution.

There are five components to the process which the Department uses to bring to notice cases believed to have a higher than average risk of incorrect payment. They are:

- statistical analysis of characteristics known to be associated with incorrect payment;
- Accelerated Claimant Matching, which is a sophisticated, computer-based system for checking overnight the authenticity of the previous day's claims and client actions which might lead to incorrect Social Security payments;



- local knowledge of the Regional Offices which "manage" the payments of persons while they are clients of the Department;
- information provided by the public which, although not sought in campaigns by the Department, is nevertheless acted on when received, and
- data-matching of client identity, income or other details with similar information from other sources. These sources are Registrars of Births, Deaths and Marriages, the Australian Electoral Commission and the Health Insurance Commission. In addition, periodic matching of identity details provided by the Department of Immigration, Local Government and Ethnic Affairs is used to detect prohibited non-citizens who have been paid social security payments incorrectly.

Data-matching is currently done by computer and manually. The manual matching is very time consuming, costly and, compared with the efficiency of modern computer matching techniques, has a low benefit to cost ratio.

The Auditor-General has referred to the usefulness of data-matching on a number of occasions, eg. Report No 24 of 1989-90.

#### Department of Employment, Education and Training

The Department of Employment, Education and Training has in place a program of pre-payment controls in which clients must substantiate certain claims made on their Austudy applications. In addition, a range of post-payment controls to detect cases of incorrect payment exist including the following:

- . enrolment/attendance checks with institutions;
- . verification of students' income with nominated employers;
- . mandatory notification of changed circumstances ("compliance exercises"), and
- . computerised internal data-matching.

As in Social Security, attention is focused upon the checking of individuals believed to be at a higher than average risk of overpayment. Where overpayments are detected, the debt must be repaid promptly and prosecution action is initiated in some cases.

The Department could not contemplate using manual systems to identify and correct these residual cases. The staffing costs involved would be prohibitive. The Government concluded that the only effective strategy for identifying and correcting the residual incorrect payments would be to employ computer data-matching techniques. The Department was aware that the technology was available to permit high speed matching of very large volumes of data.

It was estimated that these efforts could produce savings in Social Security outlays in the order of \$300m in a full financial year. A detailed dissection of the estimated savings by program type is provided at the end of this Section.

There are potential savings in the outlays of other Agencies. For example, it was estimated that introduction of the new matching program could produce savings in the order of \$30m in a full financial year in Department of Veterans' Affairs outlays. Potential savings were also acknowledged but not actually estimated in the case of Employment, Education and Training outlays, Department of Community Services and Health outlays and increased revenue to the Australian Taxation Office flowing from the identification of cases of income tax evasion.

It was estimated that through the adoption of computer matching techniques some 60,000 to 70,000 clients/claimants would have their existing payments cancelled and reductions in fortnightly rates of payment made for a further 40,000. These estimates were considered conservative. In current terms this means that approximately:

- (a) two per cent of existing unemployment, sickness and special benefit payments would be cancelled;
- (b) two per cent of sole parent pension payments would be cancelled;
- (c) one per cent of age and invalid pensions would be cancelled (and a further two and a half per cent would be subject to downward variations in rates of payment), and
- (d) two per cent of family allowance payments would be cancelled.

No account was taken of Family Allowance Supplement payments since these are already checked manually using taxation information.

Against these projected savings, implementation costs were estimated to be relatively low. The major cost involved the acquisition of new high speed computer matching equipment for the Department of Social Security. For estimate purposes this was set at \$4.5m. The actual cost will depend on the tender process. As it was known that the lead time for acquisition of the equipment would be significant, allowance was also made for the purchase of additional processing power and disks for the Department's existing Canberra mainframe so that some matching could occur and savings be made before the installation of the new equipment. The estimated cost of this upgrade was \$2.5m.



## SECTION 5: COST/BENEFIT ANALYSIS

The preceding discussion on the justification for the new matching program outlined the central elements of the arrangements. This section discusses in more detail the costs and benefits taken into account in the deliberations leading to the decision to introduce the Program.

### Financial Considerations

Income-support Agencies use risk analysis techniques to detect incorrect payments which occur as a result of clients failing to disclose changes of circumstances. For Social Security, the results of that work are set out in the Department's Annual Report.

In the 1989-90 financial year, Social Security undertook:

- . 472,100 reviews of unemployment benefit clients and cancelled 51,600 payments ie. 10.9% of the cases reviewed;
- . 149,900 reviews of sole parent pension clients and cancelled 18,600 payments ie. 12.4% of the cases reviewed;
- . 873,100 reviews of age, invalid and other pension clients and varied fortnightly payment rates downwards for 111,500 cases ie. 12.8% of the cases reviewed, and
- . 232,000 reviews of family allowance recipients and cancelled 30,400 payments ie. 13.1% of the cases reviewed.

The incorrect payments listed above were detected by targeting cases where it was believed there was a higher than average risk of incorrect payment.

If the Department focussed solely on 'the higher than average risk' population it would not detect residual incorrect payments distributed throughout the remainder of the population. For that reason, the Department ensures that, in addition to risk-based review activity, residual parts of its client populations are sampled and subject to review as well.

In the 1989-90 financial year, Social Security undertook a random sample survey of the correctness of payments to the family allowance population. The survey indicated that 2.3 per cent of the sample were being incorrectly paid because parental income exceeded allowable limits.

Based on the findings of the survey, the Department believes that the proportion of residual incorrect payments in the income-support payment populations would be in the order of 2 per cent. While this is a low percentage, the size of the overall populations is very large, standing at present at approximately four and a half million clients.

### . Department of Veterans' Affairs

The Department of Veterans' Affairs undertakes regular and selective reviews of clients to ensure the circumstances it has recorded for the clients are correct. Client details are checked against information held by other Agencies (eg Social Security, Employment, Education and Training and the Australian Taxation Office) to ensure there is no evidence of duplicate payments.

### . Department of Community Services and Health

The Department of Community Services and Health annually checks with all recipients of First Home Owners Scheme grants to ensure that they continue to own and occupy their home and therefore retain eligibility for continued payment of benefits. It also conducts computer matching exercises against its own records to detect duplicate applications and incorrect payments, as well as sample checks on information provided by applicants. Action is taken to recover any incorrect payments and, where warranted, to prosecute applicants making fraudulent claims.

### Justification for the New Program

Successive Governments have been concerned to uphold the integrity of the financial assistance programs administered through Government Agencies and to ensure that the Agencies are properly accountable for the funds they distribute. The Departments of Social Security, Employment, Education and Training, Veterans' Affairs and Community Services and Health have control measures in place to help them ensure that the payments they make are at the correct level and are made only to persons entitled to receive them.

Existing control measures, particularly some of the technical measures introduced in recent years, have been very effective. Nonetheless, opportunities remain for some people to receive payments to which they are not entitled. It is important that the funds available for financial assistance programs be directed to those entitled to them. If this is to be achieved, the integrity of financial assistance payment systems must be raised to the highest possible level.

Incorrect payments made arise either through people not advising Assistance Agencies of changes in their employment, income or living circumstances or through deliberate fraud. Many millions of Australians receive forms of financial assistance from Government Agencies. The cost of undertaking regular manual reviews of the circumstances of all these clients is prohibitive. For that reason, most Assistance Agencies have adopted a risk-based approach in their review work so that efforts are directed at clients with a higher than average chance of being incorrectly paid. Most Agencies have introduced some form of computer based data-matching which



permits the checking of client circumstances with a rapidity and efficiency which cannot be matched by labour intensive manual methods. This has been made possible through the development in recent years of new computer technologies which permit high speed matching of very high volumes of information.

The Government has decided to close remaining loop-holes in the control systems used by the Agencies paying financial assistance by:

- . extending requirements for the clients of Assistance Agencies to provide Tax File Numbers, and
- . taking advantage of the data-matching technologies now available.

The provision of Tax File Numbers will allow income information provided by clients to Assistance Agencies to be checked against income records held by the Australian Taxation Office. This cross-checking of income information will greatly strengthen the income test arrangements which apply to most financial assistance payments. Without this cross-checking it is possible for people to declare one level of income to one Agency and another level of income to another Agency. Second, the use of new high speed matching technologies will allow the matching of client information held by the various Assistance Agencies to be undertaken with a degree of efficiency and effectiveness not previously available.

This will greatly assist in the identification of cases where clients may be receiving payments to which they are not entitled from one or more Agencies. These cases cannot be identified without the cross-matching of data held by different Agencies. The cases would not exist, of course, if all clients met their obligations to inform Agencies about their true circumstances at grant and to report promptly to Agencies any subsequent change in their circumstances.

Although the percentage of the income-support population likely to be affected by the measures is low (about 2 per cent), it has been estimated that, because of the large number of people involved, these new measures could save in the order of \$300 million in a full financial year in Social Security outlays. This represents a very significant saving to the public purse and provides an assurance to the community that welfare funds are not being drained from the system by persons not entitled to them.

The objectives underlying these new measures cannot be achieved by other means. The comprehensive matching of data proposed is not feasible without the use of sophisticated computer technologies. Nor could the proposed check of income information with the Australian Taxation Office be achieved as efficiently and effectively without the use of Tax File

It would be possible to undertake the matching proposed without using Tax File Numbers, but as has been noted elsewhere, matching on keys such as name, date of birth and address is much less reliable than matching which can be based on unique identifiers such as Tax File Numbers. The more reliable the matching of income details can be made, the more effective it will be in achieving savings and the less likely it will be that incorrect matches lead Agencies to contact their clients unnecessarily.

---



#### SECTION 4 ALTERNATIVE METHODS

Other parts of this document make reference to the reasons why the Government decided to adopt a new program of data-matching between Agencies. This section summarises the arguments advanced elsewhere.

It was known as a result of a Department of Social Security sample survey of family allowance payments and through earlier experiences of matching selected data between Agencies that, despite the various control measures employed within Agencies, there was a residual level of incorrect payments which remained undetected.

Risk based control measures employed by most Agencies aim to achieve the most cost-effective and productive control arrangements by concentrating the efforts of available resources on reviewing the entitlements of clients considered to be most at risk of being incorrectly paid. Implicit in this approach is the less frequent reviewing of clients not in the categories considered to be at higher risk. It is among these clients (the majority) that the residual cases of incorrect payment reside.

To identify the residual cases it is necessary to review very large numbers of clients rather than just a sample of clients. Given:

- the many clients serviced by the Assistance Agencies (about 4.5 million clients for Social Security, about .5 million clients for Veterans' Affairs, about 1 million for Employment, Education and Training and about 120,000 clients for the First Home Owners' Scheme), and
- the even larger client base of the Australian Taxation Office (about 10 million), and the size of reference data files which may need to be consulted (eg the Australian Electoral Commission file (about 10 million records) and the Health Insurance Commission file (about 20 million records));

the task of manually reviewing the bulk of Assistance Agency clients on an individual basis and making the necessary checks against the various Agency records would clearly be an impossibility. It is considered the task would be so logistically complex and would consume the efforts of so many thousands of staff that it has not been subject to detailed costing.

If a comprehensive review of Assistance Agency clients is to be undertaken to identify residual overpayments, there is no option but to employ modern technology to match automatically the data held by various Agencies. The amounts of data involved and the complexity of the review processes proposed effectively mean that if the task is to be undertaken at all then it must employ modern computing techniques. There is simply not a range of other viable options for completing the task.

Numbers. Matching using other identity keys such as name, address, date of birth and so on is possible, but experience has shown that it is a technique fraught with imperfections. That is not to say that it cannot be cost-effective in the absence of more reliable bases for matching.

Use of Tax File Numbers for income matching purposes will produce a high degree of confidence in the results. In the system proposed, Tax File Numbers and other client information will be revealed to far fewer Agency staff than would be the case if less accurate matching systems requiring more manual scrutiny of client records were to be employed. The Privacy Commissioner has been fully briefed on this aspect as has the Senate Standing Committee on Legal and Constitutional Affairs which recommended to the Senate that the enabling legislation be approved.

The matching arrangements are to be implemented in a way which will protect the confidentiality of client information and will protect the rights of individuals who may be contacted by Assistance Agencies as a result of the data-matching. The legislation authorising the new matching arrangements contains strict privacy safeguards and these, together with the monitoring role to be adopted by the Privacy Commissioner, offer the community strong guarantees against the adoption of insensitive approaches by the Agencies involved with the new measures.

#### PROCEDURES TO BE EMPLOYED

Matching under the new data-matching program will be undertaken by the Data-Matching Agency and by the Australian Taxation Office.

The Data-Matching Agency will comprise officers of the Department of Social Security who have been directed to be responsible for the matching of data under the Data-matching Program (Assistance and Tax) Act 1990.

Officers of the Data-Matching Agency will notify Source Agencies when a cycle of matching is to begin and will ask Source Agencies to prepare files of their data in a particular format for inclusion in the data-matching process. Those files will be delivered to the Data-Matching Agency on a specified day under strict security conditions.

The steps which will comprise a matching cycle are set out in detail in Section 7 of the Data-matching Program (Assistance and Tax) Act 1990 which is at Appendix 1. The Data-Matching Agency and the Australian Taxation Office will follow those steps in conducting the data-matching for which they are responsible.



As the various steps in the data-matching cycle are completed cases of possible incorrect Tax File Numbers, identities or payments may be identified. The Data-Matching Agency will refer these discrepant cases back to the relevant Source Agency for examination. The Source Agencies will make an assessment of the information provided and decide whether or not further investigation is warranted.

When all the data-matching in a data-matching cycle has been completed the Data-Matching Agency will destroy all the data provided to it which has not led to the identification of a discrepancy. For each subsequent data-matching cycle new data will be sought from the Source Agencies.

#### NATURE AND FREQUENCY OF MATCHING

Several sorts of matching will be undertaken during a matching cycle. These are identified in Section 7 of the Data-matching Program (Assistance and Tax) Act 1990.

In Step 1 of a data-matching cycle the Data-Matching Agency will check the validity of Tax File Number information given to it by testing the numbers against an algorithm given to it for this purpose by the Australian Taxation Office. If invalid numbers are found the Data-Matching Agency will compare identity data for that number against reference identity data provided to it for this purpose by the Australian Electoral Commission and the Health Insurance Commission. Any Tax File Number data which is found to be incorrect using either of these checks will be referred back to the relevant Source Agency.

The second step in a data-matching cycle requires the Data-Matching Agency to extract from the data provided to it valid Tax File Numbers and the associated Assistance Agency identification number and pass this information to the Australian Taxation Office. (The associated Assistance Agency identification numbers are the numbers which Assistance Agencies assign to their clients.)

In Step 3 of a data-matching cycle the Australian Taxation Office uses the information given to it by the Data-Matching Agency to extract taxable income and personal identity data from its records for each person for whom it has received a Tax File Number. It will then pass this information back to the Data-Matching Agency.

In Step 4 of a data-matching cycle the Data-Matching Agency will compare the identity information given to it by the Australian Taxation Office with identity information for the same clients provided to it by the Assistance Agencies. The purpose of identity matching is to find cases of false identity in which a person claims a payment to which they are not entitled using the a bogus or incorrect identity.

In Step 5 of a data-matching cycle the Data-Matching Agency will carry out both payment matching and income matching. In payment matching, data provided to the Data-Matching Agency by Assistance Agencies will be compared to see if people are receiving inconsistent payments. For example, a person should not be receiving both Austudy and Unemployment Benefit payments at the same time.

In income matching, the Data-Matching Agency will compare taxable income details provided by clients to Assistance Agencies with taxable income details provided by the Australian Taxation Office for those same clients. The purpose of this matching is to identify cases in which clients may have misinformed one or more Agencies about their income and may therefore be receiving incorrect Assistance Agency payments or be paying less tax than they should be.

The Data-matching Program (Assistance and Tax) Act 1990 specifies that each data-matching cycle must be completed within two months of its commencement and that no more than nine cycles may be conducted each year. One cycle cannot proceed until the previous one has finished.

---



9/29/94

at-BEC

NSW Privacy Committee

(✓)

Kat St Syd

(02) 2523843

Box 6 GPO Syd 2001.

"Survey Guidelines: guidelines for Survey + Research No 42  
Nov 1979."

Copy being sent.  
Copy at BEC

(Cowell) Aust Bureau of Statistics

(02) 2684111  
8.30 / 4.30

Info Paper: Some Guidelines in the design + attainment  
of a community survey.

Cat No 1201.1

o/p.  
'94.



*Hamilton*



**PRIVACY COMMITTEE  
OF NEW SOUTH WALES**

**1992 ANNUAL REPORT**



# Privacy Committee

---



New South Wales

*With Compliments*

G.P.O. Box 6, Sydney, N.S.W., 2000    Level 12, 189 Kent Street, Sydney, N.S.W., 2000  
Telephone: (02) 252 3843    Facsimile: (02) 252 3842



The Hon. J. Hannaford, M.L.C.,  
Attorney General and Minister for Justice,  
Level 20,  
Goodsell Building,  
8 - 12 Chifley Square,  
SYDNEY, N.S.W., 2000

Dear Mr. Hannaford,

In compliance with Section 17 of the Privacy Committee Act 1975, the Privacy Committee has the honour to submit its Annual Report for the year 1992.

C. Puplick (Chairman)  
M. Tangney (Acting Executive Member)  
B. Grant  
A. Humpherson, M.L.A.  
R. Lewis  
I. Macdonald, M.L.C.  
J. Maling, A.M.  
M. Norsa  
M. Richardson  
D. Smith  
D. Temple  
B.R. Vermeesch

---



### The Privacy Committee's Goal

"The promotion and protection of the privacy of persons in New South Wales".

The Privacy Committee, a statutory body constituted under the Privacy Committee Act 1975, No. 37, works to achieve its goal by:

- \* Promoting and protecting the privacy of persons in New South Wales through the conduct of research, the provision of advice, and the preparation of reports and recommendations on privacy policy issues to the government and the community.
  - \* Promoting the adoption and implementation of privacy protection programs.
  - \* Answering inquiries and investigating allegations of breaches of privacy of persons and undertaking conciliation and resolution of complaints.
  - \* Preparing and disseminating information on privacy issues and providing educational material and media comment on topical privacy issues.
  - \* Managing allocated funds, staff and other resources to ensure efficient and effective achievement of legislative goals.
-



**THE PRIVACY COMMITTEE**

The Committee is responsible for the whole range of privacy issues in both the public and the private sectors.

Established by the Privacy Committee Act 1975 (NSW), it commenced operations on 2nd May, 1975.

It is a statutory Committee independent of government, which acts as a privacy ombudsman.

Section 5 (2) of the Privacy Committee Act states that: "The Committee shall consist of not less than twelve nor more than fifteen members" who are selected in accordance with a formula set out in the Act.

**COMMITTEE MEMBERS**

<b>Totti Cohen</b>	AM, OBE, Solicitor, Chairman*
<b>Christopher Puplick</b>	Chief Executive Officer, Packaging Environment Foundation of Australia (Chairman from June, 1993)**
<b>Jacqueline Morgan</b>	Executive Member (until January, 1993)
<b>David Dale</b>	Journalist*
<b>Helen Gamble</b>	Professor of Legal Studies, University of Wollongong*
<b>Bill Grant</b>	Deputy Director-General, Attorney General's Department**
<b>Wayne Haylen</b>	Queen's Counsel*
<b>Andrew Humpherson</b>	Government Member of Parliament (from October 1992)
<b>Les Lawrence</b>	Computer Consultant*
<b>Rod Lewis</b>	Partner, Hunt Musgrave and Peach**
<b>Ian Macdonald</b>	Opposition Member of Parliament
<b>Michael Norsa</b>	Computer Consultant
<b>David Smith</b>	General Manager, Mirror Australia**
<b>Diana Temple</b>	Associate of the Department of Pharmacology, Sydney University
<b>Andrew Tink</b>	Government Member of Parliament (until August, 1992)
<b>Bob Vermeesch</b>	Deputy Chairman, Commercial Tribunal

\* Term expired May 1993

\*\* Appointed November 1992

**STAFF OF THE COMMITTEE**

<b>Jacqueline Morgan</b>	Executive Member
<b>Maureen Tangney</b>	Director, Research and Policy
<b>Diane Johnson</b>	Investigations Officer
<b>Bruce Alston</b>	Research Officer
<b>John Gaudin</b>	Research Officer
<b>David Goodis</b>	Research Officer (from October 1992)
<b>Liz Atkins</b>	Executive Assistant
<b>Eleanor Lees</b>	Commonwealth Trainee (from December 1991)



## FUNCTIONS OF THE COMMITTEE

Section 15 (1) of the Privacy Committee Act sets out the powers, duties and functions of the Committee as follows:

- "15 (1) Subject to this Act, the Committee -
- (a) may conduct research and collect and collate information in respect of any matter relating to the privacy of persons;
  - (b) may and, if directed by the Minister so to do, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of persons;
  - (c) may make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons;
  - (d) may receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;
  - (e) may, in relation to any matter relating to the privacy of persons generally, disseminate information and undertake educational work;
  - (f) may, in relation to any matter relating to the privacy of persons generally, make public statements; and
  - (g) may, for the purposes of this Act, conduct such inquiries and make such investigations as it thinks fit.
- (2) The Committee shall, from time to time when requested by the Minister, prepare and submit to the Minister programs for the examination of matters relating to the privacy of persons and pursue those programs in such order, if any, as is determined by the Minister and notified by him to the Committee.
- (3) Any member of the Committee may submit to the Minister a minority report or recommendation on any matter in respect of which the Committee makes a report or recommendation to the Minister."

- 49b. Police Department On-Line Availability of the Criminal Names Index (August 1979)
- 50. Consumer Credit Reporting: An Overview (November 1979)
- 51. Commercial Credit Reporting: An Overview (February 1980)
- 52. \*Police Department On-Line Access to Department of Motor Transport Traffic Convictions Records (April 1979)
- 53. Telephone Usage Monitoring Systems (TIMS)(November 1983)
- 54. Acquired Immune Deficiency Syndrome (AIDS) - Guidelines for the Testing of Antibodies to HTLV-III (AIDS) Virus (February 1986)
- 55. Privacy Issues and the Proposed National Identification Scheme (March 1986)
- 56. Submission to the Joint Parliamentary Select Committee on Telecommunications Interception (September 1986)
- 57. The Medical Examination Centre (March 1987)
- 58. National Identification System - A Further Report (February 1988)
- 59. Direct Marketing - Discussion Paper (April 1989)
- 60A. Report on Regulation of Credit Reporting (March 1989)
- 60B. Further Report on Regulation of Credit Reporting (September 1989)
- 61. Privacy Law in the Information Age - Seminar Proceedings (June 1990)
- 62. Electronic Vehicle Tracking Issues Paper (August 1990)
- 63. Privacy and Data Protection in New South Wales - A Proposal for Legislation (June 1991)
- 64. Drug Testing in the Workplace (October 1992)
- 65. Private Lives and Public Health: Privacy Guidelines for HIV Testing (August 1993)



31. Guidelines for the Operation of Personal Data Systems (March 1986)
32. Submission to the Australian Law Reform Commission Regarding the Census (April 1977)
33. Submission to the Criminal Investigation Bill 1977 (Commonwealth) (May 1977)
34. Does the Privacy Committee consider that a register of pecuniary interests should be introduced? Submission to the Joint Committee of the Legislative Council and Legislative Assembly upon pecuniary interests (June 1977)
35. Research and Confidential Data: Guidelines for Access (May 1986)
36. The Medical Examination Centre (October 1977)
37. Defamation and Privacy: Submission of the New South Wales Privacy Committee on the Proposals of the Australian Law Reform Commission (Against 1977)
38. Personal Data Systems in the New South Wales Public Sector - State Electoral Office (August 1977)
- 39a. Employment Guidelines - The Privacy Aspects of Employment Practices in the Private Sector (October 1979)
- 39b. Employment Background Paper: The Privacy Aspects of Employment Practices in the Private Sector (October 1979)
- 39c. Openness in the Employee-Employer Relationship to Ensure Fairness (March 1979)
40. Consumer Affairs Motor Dealers Inspectors Access to DMT Motor Vehicle Registration Records (November 1977)
- 41a. \*The Use of Criminal Records in the Public Sector (November 1977)
42. Guidelines for Surveys (January 1978)
43. The Department of Motor Transport - Personal Data Systems in the New South Wales Public Sector (April 1978)
44. Blacklists: Finding a Fair Balance of Interests (January 1978)
45. The New South Wales Police Special Branch (March 1978)
46. \*International Legislation for Privacy Protection in Data Systems (Implications for Australia)(June 1978)
- 47b. Lie Detectors (April 1979)
- 48a. The Collection, Storage and Dissemination of Criminal Records by the Police (November 1978)
- 49a. Guidelines for Debt Collection (August 1979)

## CHAIRMAN'S PREFACE

It is often instructive to look to the past to see what progress has been made towards the fulfillment of future plans and objectives. Regrettably, for the Privacy Committee, a 10 year stroll down memory lane is not an altogether pleasing experience.

Over the last 10 years, the Committee's Annual Reports have highlighted two very serious problems - both capable of simple solution and both as yet unsolved because of parliamentary inertia.

The problems concern the lack of information privacy legislation and the lack of Committee resources. Without adequate resources, the Committee has been unable to act effectively as a conciliator, advisor and watchdog. Without proper legislation, it has been powerless to stop the large scale violations of privacy rights, as evidenced in the report of the Independent Commission Against Corruption into the Unauthorised Release of Government Information.

On the need for legislation, the Committee wrote in its 1982 Report:

*"The Committee believes that the range and extent of privacy invasions, in the area of information privacy, where most complaints arise, makes it no longer feasible to leave the bulk of privacy protection to voluntary guidelines. The potential for serious invasion of privacy is large and increasing rapidly. Legislation is now necessary, not merely as a remedial response to existing violations of privacy rights, but as a general preventative means of protecting privacy rights and laying down privacy protection standards ..."*

*The two main dangers in the area of information privacy stem from the rapid development of electronic data processing on the one hand, and the increasing powers of officialdom on the other ... The previous twenty years have seen a progressive increase in the powers of government and semi-government to demand and collect information on individuals ..."*

*This dual increase in computerisation and powers of officialdom can lead to privacy invasion on a grand scale".*

Grand scale indeed! The ICAC Report demonstrated only too well how personal information supplied in trust, and frequently under legal compulsion, is misused, bartered and sold. If effective data protection legislation had been in place in the 1980s, it would have been much more difficult for the kind of network exposed by ICAC to develop. Record keepers would have been well aware of basic data protection principles and would have been accountable fully for their use and misuse of personal information. Consequently, unauthorised access to data would have been reduced to isolated instances rather than allowed to develop to systemic proportions.

The ICAC Report demonstrated the existence of an insatiable demand from third parties for personal information which individuals have supplied to public agencies. While most major organisations implicated in the corrupt trade have taken steps to clean up their act, there can be no assurance that this trade has been eliminated or substantially wiped out.

At the same time, major government agencies which collect and process personal information are pushing ahead with new computerised systems. The Government has adopted an information technology policy to promote electronic exchange of information between agencies and efficient contracting out of computerised services.



These developments are set to raise issues of information privacy in an acute form. The absence of data protection legislation represents a significant gap in policy in this area. However, legislation is only part of the answer. Unless it is backed up by a properly resourced and independent supervisory authority, there is no point in parliament even considering a Data Protection bill.

The Committee speaks from bitter experience when it comes to the issue of inadequate resources.

In 1982, the Committee reported how it was struggling to perform its functions as its budget of \$180,000 did not meet operating expenses. It had a staff of just seven full-time employees, having being forced to eliminate one full-time position in order to cover expenses. In 10 years the only thing that has changed is that the Committee now operates with a full-time staff reduced to six!

Again in 1982, the Committee compared its budget and staff numbers with that of agencies with similar functions. It discovered that the Ombudsman's Office in 1982 consisted of three statutory officers and 35 staff and it operated on a budget of more than \$1,000,000. In the same year the Anti-Discrimination Board (ADB) had a staff of 9 and a budget of more than \$660,000.

How have these agencies fared 10 years on? In 1992, the Ombudsman's Office had grown to operating with an allocation of funds in excess of \$4,500,000 and its staff had effectively doubled to 76 (including statutory officers). In 1992, the ADB was operating with an allocation of more than \$2,000,000 and its staff had more than tripled to 33.

In pointing this out, I am not in any way suggesting that the resources of the two bodies described above are excessive. I am simply making the rather obvious point that the Committee is pathetically understaffed and underfunded in comparison with agencies that perform similar roles. Furthermore, this effective reduction in resources is accompanied by an increased workload, increased public awareness of people's rights to privacy protection and ICAC's clearly identified need for greater systematic privacy protection.

It is worth repeating the words of the Committee's former Chairman, Mrs. Totti Cohen, who reported last year:

*"In New South Wales, in stark contrast to the hundreds of millions of dollars which are invested each year in information technology, there is virtually no financial commitment to the protection of privacy. The people of this State have paid dearly for "privacy on the cheap" as evidenced by the revelations of the ICAC Report".*

I would like to record my appreciation for the contribution of Totti Cohen as Chairman (and other previous members of the Committee) and hope that, in the near future, the enactment of privacy and data protection legislation will justify the commitment she and the Committee gave from 1983 to 1993 to this important work.

Christopher Puplick  
CHAIRMAN\*

\* (Appointed June, 1993)

7. Medibank Privacy Issues (Submission Relating to the Health Insurance No. 2 Bill, 1975)(August 1975)
8. \*Defamation and the Granting of Credit (August 1975)
9. Press Councils (September 1975)
10. Rehabilitation of Offenders (June 1976)
11. \*Enforcement of Money Judgements (includes submission to the New South Wales Law Reform Commission)(October 1975)
12. Submission to the Royal Commission on Intelligence and Data Security (January 1976)
13. Problems in Consumer Credit Report (February 1976)
14. A Report on Consumer Access to Credit Bureau Records in New South Wales (April 1976)
15. Personal Data Systems (February 1976)
16. Overseas proposals Relating to the Regulation of Personal Data Systems (April 1976)
17. Programme for Study of Medical Privacy (February 1976)
18. \*Programme for Study of Privacy Aspects of Employment Practices (February 1976)
19. \*Criminal Records and their Uses in New South Wales (September 1976)
20. Research Materials held by the Committee (September 1976)
21. \*Bibliography: Extra-Judicial Debt Collection (May 1976)
22. A Summary of the Morison Report on the Law of Privacy (Tabled April, 1973)(April 1976)
23. Legislation Concerning Educational Records in the USA (August 1984)
24. Individual Identification (September 1976)
25. Mandatory Reporting of Child Abuse (September 1976)
26. Unsolicited Mail and Leaflets (September 1976)
27. \*Report on the Public Service Board Criminal Checks in Employment (November 1976)
28. Personal Data Systems in the New South Wales Public Sector Totalizator Agency Board (November 1976)
29. Unsolicited Telephone Calls (September 1978)
30. Survey of Personal Data Systems in the New South Wales Public Sector (January 1977)



## APPENDIX 2

## List of Publications

**A. ANNUAL REPORTS**

1975 - 1991

**B. THE PRIVACY BULLETIN**

Volume 1 No. 1 March 1985  
 Volume 1 No. 2 July 1985  
 Volume 1 No. 3 December 1985

Volume 2 No. 1 July 1986  
 Volume 2 No. 2 September 1986

Volume 3 No. 1 February 1987  
 Volume 3 No. 2 May 1987  
 Volume 3 No. 3 November 1987

Volume 4 No. 1 July 1988  
 Volume 4 No. 2 November 1988  
 Volume 4 No. 3 December 1988

Volume 5 No. 1 November 1989

Volume 6 No. 1 April 1990  
 Volume 6 No. 2 August 1990  
 Volume 6 No. 3 September, 1990

Volume 7 No. 1 April 1991  
 Volume 7 No. 2 May 1991

**C. REPORTS**

1. Integrated Data Systems (Commonwealth - Crisp Report)(May 1975)
2. \*The Credit Industry - Granting of Credit and Credit Bureaux (May 1975)
3. \*Australian Criminal Information Centre (May)
4. Criminal Information Systems - Submission to the Australian Law Reform Commission (July 1975)
5. Universal Identification Numbers (July 1975)
6. National Compensation Bill 1975 (August 1975)

## TABLE OF CONTENTS

## CHAPTERS:

<b>1. INTRODUCTION</b>	<b>9</b>
<b>2. ADMINISTRATION</b>	<b>12</b>
2.0 Introduction	12
2.1 Membership and Meetings of the Committee	12
2.2 Staff of the Committee	12
2.3 Committee Resources	13
2.4 Priorities	13
2.5 Delegations	14
2.6 Membership of Other Committees and Statutory Bodies	14
<b>3. PROMOTING PRIVACY</b>	<b>15</b>
3.0 Introduction	15
3.1 Media	15
3.2 Speaking Engagements	15
3.3 Publications	16
3.4 Privacy Agencies	16
3.5 14th International Data Protection and Privacy Commissioners' Conference	17
<b>4. SIGNIFICANT ISSUES</b>	<b>19</b>
4.0 Introduction	19
4.1 Report on the Unauthorised Release of Government Information	19
4.2 Data Protection Bill 1992	24
4.3 Computerised Operational Policing System (COPS)	26
4.4 Health Communications Network	27
4.5 Drug Testing in the Workplace	28
4.6 AUSTEL Inquiry into the Privacy Implications of Telecommunication Services	32
<b>5. ADVICE</b>	<b>37</b>
5.0 Introduction	37
5.1 Pre-employment Health Assessment Project	38
5.2 Pre-employment Health Assessment Form	39
5.3 Exchange of Health Related Information on Persons in Custody	40
5.4 Joint Select Committee on Gun Law Reform	42
5.5 Inquiry into an Open Births, Deaths and Marriages Registry	43
5.6 Video Surveillance and Munchausen's Syndrome by Proxy	45
5.7 Privacy and the Handling of Subpoena Documents	46



5.8	Law Enforcement Access Network	47
5.9	Privatisation of Public Hospital	48
5.10	Draft Local Government Bill	49
5.11	Privacy Guidelines for HIV Testing	51
5.12	Review of the Adoption Information Act 1990	51
5.13	Distribution of Names of Justices of the Peace	53

<b>6.</b>	<b>COMPLAINTS</b>	<b>55</b>
6.0	Introduction	55
6.1	Resolution of Informal Complaints	55
6.2	Resolution of Formal Written Complaints	55
6.3	Statistics	56
6.4	Complaints about Police	57
6.5	Some cases:	58
*	Subpoenaed Records Go Astray	58
*	Numbering Nurses	58
*	Selling Family Trees	58
*	Prisoners' Privacy	59
*	Brothel Photographs	59
*	Getting off a Mailing List	60
*	Privatising Privacy?	60
*	Garnishee Orders	61
*	Sacked for a Spent Conviction	61
*	Student Inspector	61
*	Silent Telephone Numbers	62
*	Hospital File Number	62
*	Access to RTA Records	63
*	Silent Registration Record	63

## APPENDICES

1.	Budget Expenditure and Allocation	65
2.	List of Publications	66

## APPENDIX 1

### Budget Expenditure and Allocation

	Actual Expenditure 91/92	Allocation 92/93
	\$000	\$000
Salaries Etc.	285	273
Recreation Leave	0	1
Overtime	0	0
Workers Compensation	3	3
Personal Accident Insurance	0	0
Meal Allowances	0	0
Payroll Tax	19	18
Fringe Benefits Tax	0	0
Payments in Nature of Salaries	307	295
Rent	98	118
Rates, Charges Etc	1	1
Maintenance of Buildings	0	0
Insurance	0	0
Cleaning	0	0
Travelling Expenses	3	2
Motor Vehicle Expenses	0	0
Freight, Cartage Etc	0	1
Advertising and Publicity	0	0
Books Paper Etc	8	6
Fees for Services Rendered	12	22
Gas and Electricity	0	4
Laundry Expenses	0	0
Other Insurance	0	0
Postal and Telephone Expenses	5	4
Printing Expenses	14	18
Stores, Provisions, Etc	6	3
Minor Expenses	0	1
Out of Pocket Expenses	0	0
Maintenance Contracts	0	3
Maintenance and Operating Expenses	148	183
Total	455	478



RTA policy is such that, where a member of the public or a police officer objects to the Authority releasing information from their records on the grounds that it would endanger their safety, the person can apply for a suppression order. The RTA requires a written application from the person seeking the order, as well as supporting documentation from the Commissioner of Police or a District Commander. Once an application is received, an immediate four week suppression order is granted to enable the applicant to obtain the necessary documentary support from the police. If police support is not obtained by the end of the four week period, the suppression is lifted.

Both the police and the Committee supported the complainant's application and the Committee subsequently wrote to the RTA on her behalf requesting that a suppression order be granted. The RTA granted the original order and approved a second application for a further six month extension.

## Chapter 1

### INTRODUCTION

1992 was a year in which privacy and data protection issues were placed squarely before state government policy-makers.

It brought the promise that New South Wales would finally respond to the challenge of the information age by bringing in comprehensive data protection legislation, of the type the Privacy Committee has urged successive governments to enact.

There was a growing acknowledgment that an ad-hoc response to privacy and data protection issues is no longer sustainable. The gathering pace of technological change means that a more systematic response is required; one that is best provided through the introduction of data protection legislation, backed up by a properly resourced and independent supervisory authority.

This conclusion was underlined in 1992 by the release of the report by the Independent Commission Against Corruption (ICAC) on the Unauthorised Release of Government Information. The report provided details of a massive illicit trade in personal information held by government agencies, such as the Roads and Traffic Authority and the New South Wales Police Service.

The ICAC report clearly showed that the right to privacy, specifically information privacy, has neither been respected nor protected in government and business circles and that the privacy of tens of thousands of people has been breached.

The Attorney General, Mr. Hannaford, responded to the revelations of the ICAC report by announcing that he intended to introduce the necessary privacy legislation as soon as possible, in the hope that this initiative would restore New South Wales to the position of being in the forefront of protecting the individual's right to privacy.

Government consultation with the Privacy Committee is expected to form an important part of this process. The Committee has set out a blueprint for the kind of modern legislation that is required to bring the state in line with other jurisdictions. Its research provides a sure foundation for the legislators to build upon. (See the Committee's 1991 report "Privacy and Data Protection in New South Wales - A Proposal for Legislation".)

While the year saw the Privacy Committee give priority to highlighting the need for a comprehensive privacy and data protection framework, it continued its work on a plethora of specific issues.

Activities during the year included the production of a major report on drug testing in the workplace, submissions to AUSTEL's inquiry into the privacy implications of telecommunications services, to the Commonwealth Attorney General's Department concerning the legislation governing telecommunications interceptions, and participation in the New South Wales Legislative Council's inquiry into the operation of the Registry of Births, Deaths and Marriages. Demand for the Committee's complaint investigation and resolution services continued unabated.



As usual, the Committee's activities touched on privacy issues arising in a wide variety of public and private sector contexts. In large part due to the Committee's long history of promoting awareness of privacy issues, organisations are increasingly identifying privacy issues raised within their spheres of activity, and are concerned to do the right thing with regard to these issues. Every year, many approach the Committee for guidance and advice.

Whatever the context, one prevailing theme that the Committee seeks to communicate is the importance of assessing the privacy implications of new information and surveillance technology applications before systems are established and deficiencies become more difficult, and more expensive, to remedy. A consideration of the potential impact on privacy should be an integral part of such proposals.

The alternative is to allow technology to shape society in unintended or unexpected ways to the detriment of important social values, including those of privacy, personal autonomy and freedom.

The introduction of new personal information databases, and new uses of existing databases continues with dizzying speed. Unfortunately, investment by government and by the private sector, in information technology has not always been matched by a commitment to identify and address privacy issues.

While the Privacy Committee may harbour concerns about the privacy implications of one or other new information technology application, it does not always have the resources to encourage the necessary remedial action. There is only so much that the Privacy Committee can do, with a staff of six, to raise awareness and understanding of data protection concerns.

This situation will continue until such time as data protection principles receive proper public policy recognition, in both legislative and resource terms.

There is nothing particularly mysterious or controversial about these data protection principles. People should have the right to know about, and consent to, the collection of information about themselves. They should be able to know what the information will be used for, and to whom it may be disclosed. Proper limits should be placed on this use and disclosure, consistent with the principle that personal information should generally only be used or disclosed for the purpose for which it was collected. People should have a right of access to information relating to them, and be assured that the information will be securely stored.

Many data protection principles, while being protective of individual privacy, are also simply good business and administrative practice; for example, collecting only the minimum amount of personal information that is necessary for the purpose, and retaining it for no longer than is necessary.

It is the Committee's view that broad based community understanding of, and adherence to, these principles can only realistically be achieved when they receive legislative recognition; as they have at Commonwealth level, and in a multitude of other democratic jurisdictions.

Until then organisations which consider it expedient to ignore individual privacy rights will be able to do so with relative impunity, while those with a willingness to do the right thing may face an uphill task, in the absence of adequate support and guidance.

The hospital initially argued that it was not possible to change the old file number and that it had already protected the complainant's privacy by removing all previous information.

After further discussions with the hospital, the Committee was advised that a new file had been created by the hospital's admissions officer and the old file number would no longer be used.

The complainant was informed of this fact and the matter resolved satisfactorily.

#### Access to RTA Records

A company operating a fleet of street vending vans in NSW demanded to have the company name and logo removed from a number of motor vans that were not authorized to use the logos.

A firm of solicitors engaged on the company's behalf sought vehicle registration information from records held by the Roads and Traffic Authority (RTA).

The solicitors claimed that access to such information was vital to the company's attempt to protect its trade mark; as locating and identifying the owners of the vans was seen to be the only way of detecting and preventing unauthorised use.

The Committee advised that the RTA's records are not public records and they should only be disclosed in accordance with the Committee's Data Protection Principles. These principles state that information which has been collected for one purpose should not generally be used or disclosed for another unrelated purpose without the record subject's consent or the authority of law.

Until a few years ago members of the public enjoyed almost unrestricted access to RTA records. Sometimes the purposes for which access was sought (eg debt collection) were unrelated to the reason why the RTA collected the information in the first place; namely for the administration of the motor transport system.

The Committee recognises that while some other uses of RTA records may be deemed to be acceptable to the community, this would have to be reflected in legislation which was the product of consultation with the RTA, interested parties and the community.

In the present case, the Committee believed that the existence of clear legislative guidelines would be a more effective way of dealing with this type of complaint rather than dealing with each complaint on an ad hoc basis.

#### Silent Registration Record

The complainant, who had recently re-married, wished to suppress her new name and address from drivers licence and vehicle registration records kept by the Road Traffic Authority (RTA).

The complainant was continually being harassed by her former partner and she asked the assistance of the Committee. In the past, her former partner had located the complainant by accessing RTA records.



The farmer objected to the student being present on the visit. He was concerned that private and sensitive information about his affairs could easily be distributed to other school students and/or their parents in the area.

The Committee wrote to the council informing them of the complaint. The council responded with an apology and stated that only authorised council staff would be permitted to visit the farm in the future.

#### Silent Telephone Numbers

The Committee received a complaint from a person who claimed that police had illegally gained access to his unlisted phone number.

It was suggested by the complainant that his phone number had been obtained by police for the purpose of harassing him.

The Committee wrote to the Assistant Commissioner of Police. As the complaint contained allegations about police misconduct, the Police Service was required under the *Police Regulation (Allegations of Misconduct) Act* to notify the Office of the Ombudsman.

The Police Service stated that the complainant had pleaded guilty to two criminal charges and was awaiting sentence. A solicitor from the Department of Public Prosecutions had made several attempts to ascertain the complainant's legal representative in order to inform him of a new date for his court appearance. Having failed to contact his legal representative, an attempt was made to contact the complainant directly. Inquiries were then made through the correct channels and in accordance with correct procedures to obtain the complainant's telephone number. The Detective in charge of the case contacted the complainant to advise him of the new date of his court appearance.

The Ombudsman was satisfied that there was no evidence of police misconduct and no need for further investigation by his office.

The Committee was also satisfied with this finding and advised the complainant accordingly.

#### Hospital File Number

The complainant was concerned that a hospital file containing her old name (she had since changed her name by deed poll) had been activated upon her admission as a patient.

The complainant was afraid that information in the old file might be inadvertently disclosed to reveal her previous name and other sensitive information.

The Committee contacted the hospital and was advised that the old file number had been activated because the complainant had previously been a patient and had advised the hospital of this during her current admission. The contents of the old file had been physically shredded because the information was more than ten years old and there was no statutory requirement to keep the information. Computer records did not contain any reference to the patient's previous treatment and only new information was being added to the file under the old file number.

Ultimately, data protection has to become a core value, an integral part of the way in which things are done in New South Wales. The enactment of data protection legislation is the only way to ensure that this message is sent. The challenge is to create an environment in which citizens can be assured that their personal information will be treated fairly. The Privacy Committee looks forward to contributing further to this outcome.



## Chapter 2

## ADMINISTRATION

2.0 Introduction

Privacy Committee members are appointed by the Governor on the advice of the government of New South Wales. The Committee consists of no less than 12 and no more than 15 members. The Act provides for one member to be the Executive Member of the Committee. Of the appointed members, one must be a Government member of Parliament and one must be an Opposition member of Parliament, two must be employees of universities and no more than two are to come from the New South Wales public service.

The Committee's powers cover both the public and private sectors. They are set out in section 16 of the Privacy Committee Act 1975, and include the power to require any person to attend and give evidence or produce documents. In conducting any inquiry or investigation, the Committee has the powers, protections and immunities conferred on a Commissioner by Division 1 of Part II of the Royal Commissions Act 1923. The Privacy Committee has no power to enforce its recommendations, but may make reports to Parliament under sections 17 and 18 of the Privacy Committee Act 1975.

2.1 Membership and Meetings of the Committee

Mr. Andrew George, Deputy Director General of the Attorney General's Department resigned from the Committee in December, 1991 to take up the position of Magistrate of the Local Court.

In August 1992, Mr. Andrew Tink, M.P., resigned from the Committee because of increased Parliamentary commitments as a result of being appointed Chairman of the Public Accounts Committee. Mr. Andrew Humpherson, M.P. was appointed to the Committee as Mr. Tink's successor as the Government representative in October 1992.

Four additional appointments were made to the Committee in November 1992. The new Members are Mr. Bill Grant, Deputy Director General of the Attorney General's Department, Mr. Rodney Lewis, Solicitor, Mr. Christopher Puplick, Chief Executive Officer, Packaging Environment Foundation of Australia and Mr. David Smith, General Manager, Mirror Australian and Telegraph Publications.

In December 1992, the Executive Member, Dr. Jacqueline Morgan, announced that she would be retiring from the Committee at the end of January 1993.

2.2 Staff of the Committee

The Committee's full-time staff complement of six, remained unchanged during 1992.

Staff members are required to investigate complaints, undertake research and provide advice on privacy issues and also to undertake clerical and administrative tasks.

## Garnishee Orders

When a judgment debt is unpaid, the creditor can garnishee money from people who owe money to the debtor, such as the debtor's employer. In this way the debt is paid by direct deductions from a person's wage or salary.

In this case, a garnishee order was sent to a person in an ordinary window-faced envelope not unlike those used and received by his employer. The complainant was concerned to protect his privacy because the order was mailed to his work address and the name on the envelope was similar to that of another employee. The letter might easily have been opened and read by another person.

The Committee investigated the complaint. It found no breach of privacy in sending such correspondence to a place of work so long as nothing outside the envelope indicated that the letter referred to a bill for an outstanding debt.

## Sacked for a Spent Conviction

The complainant alleged that she had been dismissed from part-time employment with the Department of Corrective Services because her criminal record (a minor one) had been disclosed to the Department, contrary to the *Criminal Records Act 1991*. That Act entitles people who have committed certain minor offences to treat the convictions as spent after a ten year crime-free period. When a conviction is spent, the person who was convicted does not have to disclose the spent conviction to any person for any purpose.

The complainant alleged that the Department had written to her suggesting that she had neglected to supply the relevant information about her criminal record and that her services would be terminated accordingly.

The Committee investigated the complaint and was told by the Department that the complainant's services were in fact terminated because of her criminal record, but that at the time of the dismissal, the Department was unaware of its obligations under the *Criminal Records Act 1991*. The Department also claimed that additional reasons had been given for the sacking.

The complainant lodged an unfair dismissal action against the Department which was successful on the grounds that the Department had acted improperly in sacking her because of her record.

The Committee was satisfied that the Department had acknowledged its error in failing to adhere to the provisions of the *Criminal Records Act 1991*.

## Student Inspector

The complainant, a poultry farmer, received an inspection visit from a council health inspector accompanied by a work experience student.

Under Local Government Regulations, health inspectors have the power to enter a persons property for the purpose of carrying out regular health inspections.



### Getting off a Mailing List

The complainant had made at least 20 phone calls to a company requesting them to stop sending him unsolicited mail. The company specialises in marketing its products using mailing lists based on prospective and previous customers. New customers who purchase items are urged to place their name, and the names of their friends on a mailing list for future sale catalogues.

On each occasion the complainant called, the company promised that his name would be removed.

The complainant eventually contacted the Committee complaining of a breach of privacy.

The Committee wrote to the company requesting them to remove the complainant's name from their mailing list and to provide it with information as to how his name was originally supplied to them.

The company assured the Committee that the name had been supplied by friends of the complainant who had bought some of the company's products and that the complainant's name had already been removed from their mailing list.

The complainant continued to receive mail despite the company's assurances to the Committee. The organisation was again requested to remove the particulars and was advised that further action would be considered by the Committee if another complaint was received.

The name was removed from the mailing list.

### Privatising Privacy?

As part of the government's plan to privatise the Government Insurance Office the Premier of NSW wrote to all policy holders explaining how and why the government had chosen to privatise the company.

The complainant wrote to the Committee objecting that her privacy had been breached by the Premier gaining access to her name as part of the government's mailing campaign.

The Committee wrote to GIO asking them to advise if personal information relating to GIO policy holders had been disclosed, and if so, in what form the information had been disclosed.

GIO advised the Committee that letters to GIO policy holders (the same as the one the complainant had received) had been sent to all GIO policy holders throughout Australia. These were sent at the government's request and with the agreement of GIO.

GIO further advised that the addressing and mailing of the letter had been done 'in-house' and no personal information whatsoever had been provided to the government or to the Premier.

The Committee wrote to the complainant outlining this information. The matter was considered to be resolved.

Throughout 1992, Dr. Jacqueline Morgan and Ms. Maureen Tangney continued in their respective positions of Executive Member and Director of Research and Policy. Ms. Diane Johnson continued as the Investigations Officer. The Committee's Research Officers were Mr. Bruce Alston and Mr. John Gaudin. Secretarial assistance was provided by Ms. Liz Atkins, the Executive Assistant.

Ms. Penny Quarry who was seconded from the Attorney General's Department in March 1991 returned to the Department in January 1992. Ms. Eleanor Lees, a trainee office assistant under the Australian Trainee System worked for the Committee until November 1992.

October 1992 saw the commencement of a one year international exchange of staff with the office of the Information and Privacy Commissioner/Ontario, Canada. Mr. Bruce Alston left for Toronto to work for the Commissioner, and Mr. David Goodis arrived to join the Committee's staff for the period of the exchange.

### 2.3 Committee Resources

Last year the Committee reported that it was allocated a budget of \$474,000 for the year 1991/92.

In 1992/93 the Committee was allocated the sum of \$478,000. The budget allocation and the expenditure for the previous financial year are set out in Appendix 1.

As noted in previous years, the Committee's budget is so lean there is really no scope to meet basic expenses associated with upgrading equipment, employing temporary staff and reprinting reports when existing stocks run out. With such limited resources, the Committee always finds it difficult to meet the requests for assistance and advice made by the community.

### 2.4 Priorities

The Privacy Committee has adopted the following criteria to guide its evaluation of work priorities:

- \* The Committee should not unnecessarily commit resources to projects already being undertaken by other organisations and interest groups;
- \* The project should be effective in terms of:
  - resources (including ability of staff, timeliness of advice/report, relationship with other current or completed projects);
  - degree of impact on privacy intrusive activities;
  - increased community awareness and capacity of individuals to protect their own privacy interests.
- \* The project should relate to a matter affecting privacy which is of concern to the community.
- \* The project should address developments in technology which raise important privacy issues.



- \* The project should relate to a government initiative or have been referred by a Minister for a Department.
- \* The project involves a matter which has the potential to affect the privacy of a significant proportion of the citizens of New South Wales.

During the year three major projects received priority. These were the review of recordkeeping practices of the Special Branch of the Police Service, the development of the Computerised Operational Police System (COPS) and drug testing in employment and sports.

## 2.5 Delegations

Section 14 of the Privacy Committee Act 1975 permits the delegation of any of the powers, authorities, duties or functions of the Committee. Delegation of the Committee's powers to compel testimony and/or the production of books or documents is only permitted with the approval of the Minister. With the Minister's approval, the Committee delegated these powers to both the Chairman and the Executive Member. The Committee did not use its powers under section 14 during the reporting period.

## 2.6 Membership of Other Committees and Statutory Bodies

### Australian Statistics Advisory Council

The Executive Member, Jacqueline Morgan, is a member of the Australian Statistics Advisory Council (ASAC). The function of the Council is to advise the Treasurer and the Australian Statistician on priorities and programs of work to be adopted in relation to the provision of national statistical services.

The Council's advice to the Australian Bureau of Statistics draws upon the wide spectrum of interests and expertise of its members. Privacy has been recognised as an area requiring particular attention.

Dr. Morgan was appointed to the Council for a further term of 3 years in March 1992.

### Centre for Conflict Resolution

The Macquarie University established during 1991 a Centre for Conflict Resolution within the School of History, Philosophy and Politics.

The Executive Member, upon invitation, became a member of the Advisory Board of the Centre, and attended meetings throughout 1992.

### Consultative Group on the Credit Reporting Code of Conduct

The Privacy Committee was invited by the Federal Privacy Commissioner to join a Consultative Group for the development of a Code of Conduct on credit reporting, as required by section 18A of the Privacy Act 1988.

The Investigations Officer, Ms. Diane Johnson, represented the Committee at meetings of the Consultative Group throughout 1992.

So far as the Committee can establish, some companies involved in this form of publishing simply gather together large lists of family names from public records in order to market their products. As long as the information is obtained from publicly available records, there is little action that can be taken; although it is the Committee's view that where possible a person should be able to opt out of the publication if they choose.

The Committee spoke to the company and the complainant's request was agreed to as the print run had not yet commenced.

## Prisoners' Privacy

A complaint was received from a prisoner in the Witness Protection Scheme regarding the security of inmate files containing information about prisoners and their families.

The complainant was concerned about the adequacy of existing security measures to protect personal information relating to prisoners' families from unauthorised disclosure or misuse.

The complainant was also concerned that the information held within the prison complex could be accessed by other inmates.

The Committee contacted the Superintendent of the prison and was advised of the security arrangements. The Committee was satisfied that adequate protections were available for sensitive information.

## Brothel Photographs

The complainant contacted the Committee about a problem arising from her former place of employment.

She advised that some time ago she had briefly been employed as a receptionist in a brothel. During the period of her employment, a photograph of her was taken with the staff and this had been placed in a prominent position in the building.

Despite the complainant no longer being employed by the brothel, the photograph remained on display.

The complainant was greatly concerned by the possibility that people she knew might attend the brothel and form a mistaken impression of her employment.

The complainant spoke to the brothel owner but her request to remove the photograph was refused.

The Committee made contact with the company's solicitor and through negotiations it was agreed that the offending photograph would be removed.

The complainant was greatly relieved when informed.



## 6.5 Some cases

### **Subpoenaed Records Go Astray**

The complainant, a medical practitioner, wrote to the Attorney General over his concern that a patient's medical records had been sent to a hospital instead of being returned to her suburban practice.

The records had been subpoenaed by the District Court as part of a hearing involving an insurance claim. The doctor was upset that details of the records had probably been seen by many people before the hospital realised that the records should have been returned to her.

Upon investigation, the District Court of New South Wales (Civil Registry) conceded that the records had inadvertently become attached to hospital records which had also been subpoenaed for the same case.

The complaint was noted in the Local Courts Circular which suggested that officers give special attention to confidential items which are to be returned after subpoena.

The Committee was satisfied with this explanation and outcome.

### **Numbering Nurses**

The director of a home nursing service objected to a requirement by a medical benefits fund that the registration number of a nurse attending a home visit must be included on the patients' accounts if the patient is a member of the fund.

The director of the service felt that the inclusion of this information had invaded the privacy of her nurses.

The Committee investigated the complaint and it was subsequently found that the insurance fund had made a mistake in deeming the nursing service to be a hospital.

The matter was resolved and the fund no longer requires the production of registration numbers of nurses to be recorded on patient's accounts.

### **Selling Family Trees**

The complainant received a letter from a direct marketing company which specialises in genealogical publications.

The company had contacted the complainant in relation to the proposed publication of a book about the family heritage of people who shared her family name.

The complainant contacted the Committee requesting that her name and address be removed from the database and that her family's details not be included in the publication.

## Chapter 3

### **PROMOTING PRIVACY**

#### 3.0 Introduction

Educating the community about why privacy is important and how privacy can best be protected is the Committee's most important task. The Committee endeavours to promote privacy through its contacts with the media, by providing speakers for conferences and seminars and by distributing educational literature such as the Privacy Bulletin and the Committee's reports.

The Committee, too, needs to be educated. It is vital for the Committee to keep informed about developments in technology, policy and the law which may have implications for privacy. The Committee's contact with other privacy and data protection agencies within Australia and throughout the world frequently alerts the Committee to issues which will need to be addressed sooner rather than later.

#### 3.1 Media

The media sought the views of the Privacy Committee on many occasions throughout the year, and the Committee's activities and policies were covered in the press, and on radio and television.

#### 3.2 Speaking Engagements

The Committee is frequently asked to participate in seminars in order to provide the privacy perspective on particular issues. The Committee sees this work as an important aspect of its educative function, and endeavours to meet as many requests as possible. The Executive Member and staff members spoke at seminars and meetings on many occasions during the year, including the following:

- \* Workers Education Association, "Privacy and Data Protection Law".
- \* Institute of Personnel Management Australia Inc., "Privacy and Employment".
- \* Current Affairs Study Centre, Seminar on "Privacy, Credit Reporting and NSW Data Protection Bill".
- \* Second National Conference on Corrections Health "The Limits of Confidentiality within the Prison System".
- \* St. Vincent's Hospital - Seminar, "Privacy and Data Protection in Health Information".
- \* Independent Commission Against Corruption "Just Trade", Seminar on the Unauthorised Release of Government Information.



- \* Human Rights Centre, University of New South Wales and Privacy International, Seminar on "Privacy Regulation - International Developments, Australian Implications".
- \* Fourteenth International Data Protection and Privacy Commissioners' Conference.

### 3.3 Publications

The Committee has produced many reports and publications since its formation.

The publications are distributed to the Parliament, the Attorney General, government departments, private sector organisations and to members of the community.

A complete list of published reports is provided in Appendix 2 of this Report.

In addition, the Committee has prepared a number of submissions and papers on specific privacy issues. Copies of these submissions and papers may also be made available to the public. Submissions and reports prepared in 1991 included:

- \* Submission to the Commonwealth Attorney General's Department concerning the Review of the Telecommunications (Interception) Act 1979.
- \* Submission to the AUSTEL Inquiry into the Privacy Implications of Telecommunications Services.
- \* Comment on the Exposure Draft Local Government Bill.
- \* Drug Testing in the Workplace (Report No.64, October 1992).

### 3.4 Privacy Agencies

Bi-annual meetings of Australian privacy agencies have been held since early 1990. These meetings are attended by representatives of established privacy agencies, as well as by representatives of State Governments which are interested in enacting privacy laws. At these meetings each agency presents a report on current activities and developments affecting privacy within their jurisdiction. Agency reports are then followed by discussion of privacy and data protection issues of common concern.

The first meeting for 1992 was held in Brisbane and was sponsored by the Queensland Department of Justice. Issues discussed at that meeting included the proposed Law Enforcement Access Network, the South Australian Privacy Bill, proposals for data protection legislation in New South Wales, the Victorian Law Reform Commission's options for privacy regulation, the Census, and privacy and archives.

Mr. Bruce Slane, the newly appointed Privacy Commissioner of New Zealand, outlined the progress of the Information Privacy Bill which was expected to be passed in 1993.

As noted in last year's Annual Report, the Federal Privacy Act was amended in 1991 to regulate credit reporting practices. For this reason, the Committee was able to refer most of the credit related enquiries to the Federal Privacy Commission.

The rest of the enquiries and complaints concerned issues as diverse as drug testing, identification numbers and cards, privacy rights of tenants, telephone information monitoring systems, privacy and the media, and confidentiality of records.

### 6.4 Complaints about Police

It is worth pointing out that the Privacy Committee is not the only agency in New South Wales to receive privacy-related complaints against police officers. The Office of the Ombudsman also receives this type of complaint due to the operation of the Police (Allegations of Misconduct) Act 1978.

When allegations of misconduct are made against police officers (including misconduct which involves a breach of privacy) they must be investigated in accordance with the provisions of the Police (Allegations of Misconduct) Act. Under this Act, the Police Service is required to notify the Ombudsman whenever a complaint of misconduct is received. This includes any complaint brought to its attention by the Privacy Committee. The Police Service conducts the initial investigation into the complaint and the Ombudsman may investigate further if he considers the initial investigation was not conducted properly.

The Committee was concerned that it was not getting an accurate picture of the extent to which privacy-related complaints were being made against police officers. To resolve this problem the Committee approached the Ombudsman who agreed to provide it with non-identifying details of privacy-related complaints received by his Office.

The Ombudsman advised that, in 1992, his Office received a total of 106 complaints against police which related to privacy. Forty-six of these complaints were internal police complaints, that is complaints by police officers or arising during a police internal investigation. The internal complaints included 25 relating to the unauthorised release of confidential government information, which was the subject of an inquiry by the Independent Commission Against Corruption at the time.

The privacy-related complaints notified to the Committee by the Ombudsman can be categorised as follows:

Improper or inappropriate release, sale or supply of information	88
Improper access to information	8
Improper public and media statements	7
Defamatory statements by officers	3
	----
	106
	=====



Many complaints are resolved at this stage either by explaining the reasons for the action to the complainant, or by making the person complained about aware of the privacy issues and the effect of his or her action. If a complaint cannot be resolved by negotiation between the parties the Committee may prepare a report containing its recommendations regarding the dispute. By giving the report to the parties they are better able to understand the reasons for the Committee's decision, and, as a result, are usually more ready to accept its recommendations.

If the Committee's recommendations are not accepted, the Committee may exercise its discretion to prepare a special report to Parliament. The Committee has not found it necessary to exercise this power in the year under review.

### 6.3 Statistics

2569 complaints and enquiries were received by the Committee in 1991. Of these, approximately 2424 were dealt with over the telephone.

Files were opened on 129 written complaints and 50 were carried over from previous years. Fifty-nine of these complaint files were closed and resolved to the satisfaction of the complainant. Twenty-six were closed where the Committee believed a satisfactory resolution was achieved, even though the complainants remained unsatisfied. Twelve were found not sustained. In four complaints the Committee's recommendation of a policy change was adopted. These policy changes concerned the criminal record checking procedures of a government agency; the property inspection policy of a local council; the procedure for handling subpoenaed material by a government agency; and the publication policy of a company involved in direct marketing. Seventeen files were referred to another agency and sixty-one were carried forward into 1993.

The following list shows the main categories of written complaints received in 1992. The 1991 figures appear in parentheses.

*	20%	(20%)	Direct Marketing;
*	10%	(5%)	Debt collection methods;
*	8%	(17%)	Credit related;
*	7%	(8%)	Employment;
*	7%	(2%)	Surveillance;
*	6%	(5%)	Banks;
*	6%	(3%)	Medical;
*	5%	(4%)	Disclosure/Local Government/RTA;
*	5%	(5%)	Adoption;
*	4%	(5%)	Police methods/criminal records.

The main types of telephone complaints and enquiries received by the Committee in 1992 are listed below. Again, the 1991 figures appear in parentheses.

*	13%	(13%)	Employee privacy;
*	11%	(-)	Privacy/data protection legislation;
*	11%	(16%)	Credit;
*	10%	(9%)	Direct marketing;
*	7%	(5%)	Criminal records;
*	5%	(9%)	Surveillance;
*	5%	(4%)	Medical records.

A second meeting was not held in the latter half of 1992. Instead, the national privacy agencies sent representatives to the 14th International Data Protection and Privacy Commissioners' Conference which was held in Sydney in October.

### 3.5 14th International Data Protection and Privacy Commissioners' Conference

In October 1992, Sydney was the venue for the 14th International Data Protection and Privacy Commissioners' Conference. This was the first time the Conference had been held in Australia, and it was chaired by the Federal Privacy Commissioner, Mr. Kevin O'Connor.

The Conference was attended by representatives from Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Hungary, Ireland, Japan, Luxembourg, Netherlands, New Zealand, Portugal, Singapore, Sweden, the United Kingdom and the United States of America.

Topics covered at the Conference included developments in privacy law in the Asia-Pacific Region, progress on the European Community draft directive on data protection, health privacy issues (including genetic privacy), workplace privacy, and the practical implementation of telecommunication privacy policies.

The keynote address was given by the Federal Data Protection Commissioner of Germany, Dr. Alfred Einwag. Dr. Einwag gave an account of the problems associated with providing access to the files of the former Ministry for State Security, the so-called "Stasi files".

The Ministry for State Security was a secret service organisation which systematically compiled information on some 6 million Germans by the use of informants and collaborators, telephone taps and audio and visual surveillance devices.

Upon the re-unification of Germany, it was decided that access to the "Stasi files" would be permitted under the detailed provisions of the Stasi Files Act. By October 1992, more than 300,000 file subjects had requested access to files.

Dr. Einwag illustrated some of the repercussions of providing access to the files. Several newly elected persons resigned their seats in Parliament. Senior officials in political parties had to step down. One member of the German Parliament committed suicide after it was revealed that, some time ago, he collaborated with the Stasi. It was also disclosed that the husband of a present member of Parliament had supplied the Ministry for State Security with information on his wife for a long time.

Dr. Einwag summed up the challenge presented by Stasi files with the following words:

*"Doing justice to the victims of a regime of injustice, doing as little damage as possible to the internal peace of the nation and giving willing, former ... collaborators a chance is a task that almost exceeds human strength".*



Another address which attracted considerable interest at the Conference was that given by Mr. Ian Temby, Q.C., Commissioner of the New South Wales Independent Commission Against Corruption (ICAC). Mr. Temby provided a detailed account of the ICAC's report on the "Unauthorised Release of Government Information" (August 1992).

A number of conference participants commented that if New South Wales and Australia had had adequate data protection laws and an effective enforcement regime in place, the massive invasion of privacy exposed by ICAC may have been prevented.

## Chapter 6

### COMPLAINTS

#### 6.0 Introduction

A major statutory function of the Committee is the investigation of complaints. The Committee's complaints function serves four purposes:

1. to resolve complaints;
2. to identify areas where improvements in practices and laws relating to privacy are needed;
3. to draw Committee policy to the attention of those who are breaching privacy; and
4. to provide information which may dispel unjustified fears.

In order to ensure that the Committee's limited resources are allocated fairly and efficiently, the Committee has resolved that, in general, it will decline to investigate complaints in the following circumstances:

1. where the complaint does not relate to privacy;
2. where another body is already investigating the complaint;
3. where another body is available to investigate the complaint and it would be more appropriate for that body to investigate the complaint; or
4. where there is adequate legal redress available to the complainant.

#### 6.1 Resolution of Informal Complaints

The Committee receives a high volume of telephone enquiries many of which are resolved without the requirement to lodge a written complaint. Approximately 2424 telephone enquiries were received during the year, an increase of almost 14% over the previous year.

People with complaints related to common privacy problems are provided with a statement of Committee policy or an information brochure explaining the steps they may be able to take to resolve the complaint themselves.

A general information brochure has been prepared which includes advice on how to have your name removed from a mailing list, how to deal with unsolicited telephone calls, bag searches by store employees, spent criminal records, and how to get fingerprints or police photos destroyed.

#### 6.2 Resolution of Formal Written Complaints

When a complaint is received, the person or body complained of is given details of the complaint and asked to comment on the alleged facts and privacy issues.



### Public Lists of Justices of the Peace

The Committee was informed that there are currently no publicly available lists of Justices of the Peace and that the purpose of making such lists available would be to assist people to locate Justices of the Peace in the event they require their services.

The Committee suggested that provided the individuals concerned gave their informed consent to the inclusion of their details on such a list, then publication would be acceptable from a privacy perspective.

The Committee recommended that, the information would best be supplied in the form of lists of Justices of the Peace made available for *inspection only* purposes. This would minimise the potential of information being used for other purposes without consent.

The Committee considered that a "Yes" response to the question:

*"Do you consent to having your name and address placed on a roll released for the information of the general public".*

did not indicate informed consent to disclosure of information about newly appointed Justices of the Peace to the various justices associations.

The Committee recommended that, except where individuals have given specific consent to disclosure to particular named associations, then those associations should be in no better position than members of the general public in relation to obtaining information from the Department.

## Chapter 4

### SIGNIFICANT ISSUES

#### 4.0 Introduction

This Chapter sets out some of the significant issues of 1992. The issues examined include the scandalous state of lack of protection for information privacy in New South Wales, the development of new computer and telecommunication systems which are likely to have a significant impact on privacy, and the latest threat to employee privacy, workplace drug testing.

#### 4.1 Report on the Unauthorised Release of Government Information

In August 1992, the Independent Commission Against Corruption (ICAC) released its long awaited report on the Unauthorised Release of Government Information.

The three volume report reveals a widespread practice of corrupt conduct, based largely on bribery of public officials, and involving hundreds of people, and millions of dollars. The report clearly shows that the right to privacy, specifically information privacy, has neither been respected nor protected in government and business circles.

It shows how private investigators (many of them licensed) were lying to, and bribing, public servants and police officers to obtain information their clients wanted. The information sought included addresses, silent telephone numbers, bank account and pension details, social security information, medicare records, criminal history information and details of people's movements in and out of the country. The clients of the private investigators included some of the largest financial, banking and insurance institutions in the country.

In all, Assistant Commissioner Roden found that 155 people were found to have acted corruptly, and 101 were found to have allowed, encouraged or caused corrupt conduct. He feared, however, that this was only the tip of the iceberg as the affairs of many thousands of licensed private inquiry and commercial agents had not been investigated by ICAC.

The 14 recommendations made in the ICAC report were directed - quite properly - to the elimination of corrupt conduct and they do not pretend to be a complete answer to the privacy issues identified in the report. However, 13 of the recommendations, if implemented, would have an impact on the protection of individual's privacy rights.

#### Recommendation 1 - Information Policy

The ICAC report recommends that a policy be developed in respect of all government-held information. The policy should determine what information is to be publicly available, and what information is to be protected. This policy should have due regard for, among other things, the basic privacy principle that when information is provided for a specific purpose, it should generally be used only for that purpose, and disclosed only to persons who need it for that purpose.



According to ICAC the policy should be applied consistently and uniformly, and not left to individual departments and agencies. Any exceptions to the policy should be formalised and an end should be put to all unofficial arrangements by which government information is shared or exchanged.

As outlined in its report *"Privacy and Data Protection Law in NSW - A Proposal for Legislation"* (No.63, 1991), the Privacy Committee believes that the information policy for New South Wales should be formulated in data protection legislation.

The Privacy committee agrees strongly with ICAC that individual departments should not be allowed to draw up their own exceptions to information policies and laws. Where exceptions are allowed, for example, for law enforcement purposes, the exception should be formalised and backed up with legal authority.

The legal authority could take the form of a specific - not general - exemption under data protection legislation or it could be provided for in a Code of Practice issued under the legislation.

The Data Protection Bill which lay on the table of State Parliament throughout 1991 and 1992 provided for the development of Codes of Practice which "generally conform" with the Data Protection Principles. However, it would vest broad authority in public service department heads to devise their own Codes of Practice and to determine which people and what information would be exempt from all or any of the Codes or Data Protection Principles. In the Committee's view this approach would produce nothing but inconsistency across the public sector.

#### Recommendation 2 - Release of Publicly Available Information

The ICAC report recommended that all information which is available to the public should be made readily quickly and cheaply available. This recommendation arises from its finding that even when information was legally available, privacy investigators preferred to purchase it corruptly if it could be supplied more quickly and cheaply.

The report also considered the issue of whether debt collectors should be given privileged access to address information held by Government agencies. The report concluded:-

1. There ought not to be a special rule allowing access to government information, for debt collection and related or similar purposes.
2. There ought not to be a special rule allowing private inquiry or commercial agents access to such information, whether for limited purposes or generally.
3. Subject only to the special position of law enforcement agencies and other exceptional overriding public interests, the rule relating to government-held addresses should either be that they are all held as confidential and protected, or that they are all publicly available; irrespective of the department or agency by which they are held, the purpose for which they are required, or the person by whom they are sought.

But the Committee had reservations about two issues; the propriety of reintroducing areas of broad administrative discretion in legislation defining rights to information; and, the provision of information which goes beyond that necessary to identify and locate parties to an adoption where this would involve unnecessary intrusion on the privacy of the person concerned.

The proposed discretion of the Commissioner to release information to parties outside the terms of the Act could involve a conflict with the Committee's data protection principle number 10. This principle seeks to limit disclosure of personal information to defined exceptions, including where specific legal provisions exist, where the party consents, or where there are pressing health and safety issues. The Committee believes that any grant of discretionary power should be expressed within a legislative framework which is consistent with the Committee's data protection principles.

With respect to the issue of extending the provision of non-identifying information beyond that which is available under existing provisions, the Committee believes that any further extension which allows sensitive medical or social information to be released could lead to the invasion of privacy of a party who wishes such information to remain confidential.

At the end of 1992, the Committee was awaiting further developments.

#### **5.13 Distribution of Names of Justices of the Peace**

Justices of the Peace are appointed by the government in an honorary capacity to administer oaths and take statutory declarations and affirmations and exercise other minor semi-judicial functions.

Some Justices of the Peace provide services from their home residence, while others provide services in the workplace.

In January 1992 the Minister for Justice introduced a number of changes to the Justice of the Peace system. One of these changes is that persons must establish that a community or employment based need exists for a person to be nominated. Members of Parliament are able to nominate persons for appointment, but they are often unaware of how many Justices already reside in their electorate.

The Department of Courts Administration, which maintains a list of Justices of the Peace, sought the Committee's advice about the disclosure of information from the list. The Department wanted to know whether it was appropriate to provide a list of all new Justices to the various Justices associations; whether lists should only be provided with the names of those who consented to having their name released when applying for appointment; or whether a locality list of Justices of the Peace could be displayed in a public area with the names of those who consented to having their name released for public information.

Data protection principles provide that personal information should not generally be disclosed unless the individual concerned has consented to the disclosure or the disclosure is required by law. The Committee therefore suggested that disclosure of information on individual Justices of the Peace should only be made with the consent of the individuals concerned.



In December 1991 terms of reference were drawn up for the New South Wales Law Reform Commission (NSWLRC) to inquire into and report on the Act. As part of this process, the NSWLRC wrote to the Committee seeking advice on the possibility of conducting research into peoples' experience of the operation of the Act.

The Commission believed that in order to obtain a balanced view about how the Act was working, a direct approach to people who had applied for a birth certificate and to people who had applied to have their name placed on the Contact Veto register would be one way of seeking more accurate and informed information about how the Act was functioning.

It was proposed that contact would be initiated by letter or phone call from DOCS asking people whether they wished to participate in the survey.

The Committee noted that since the Act was passed, the Committee had received many complaints and inquiries from parties to adoptions, many of whom were concerned about the release of their personal information.

It was also noted that a number of complainants have maintained their anonymity or requested strict confidentiality when approaching the Committee. This suggested that any approach by DOCS on behalf of the NSWLRC would be considered a serious invasion of privacy by people who are particularly sensitive to the issue of anonymity.

If research subjects were contacted without prior consent using information held by DOCS or the Registry of Births Deaths and Marriages, the survey would be likely to have a poor response rate as well as cause serious breaches of privacy. The Committee also anticipated that such research would almost certainly result in complaints being made to the Committee.

The Committee acknowledged that research using volunteers or persons who had previously consented to being contacted may not achieve the same unbiased results as those able to be achieved using other methods. However, it would be more acceptable in terms of minimising the risk of breach of privacy.

On the whole, the Committee did not see that the potential benefits of the NSWLRC's research proposal would outweigh the potential invasion of privacy as a result of carrying out such research.

#### Comment on the Law Reform Commission's Report

In early October 1992, the NSWLRC released its Report on the *Review of the Adoption Information Act 1990*.

Consistent with the Privacy Committee's advice, the NSWLRC decided to abandon the use of the research methodology which had been proposed to the Committee due to the serious privacy issues raised by the Committee.

Having analysed the Report, the Committee submitted a detailed comment to the New South Wales Attorney General's Department on the fifteen recommendations made by the NSWLRC.

The Committee generally supported the Report and welcomed the proposed amendments which would increase public awareness of the way personal information can be accessed and provide some reassurance to those who fear the consequences of such access.

The Privacy Committee is totally opposed to any suggestion that address information be made publicly available, irrespective of the department or agency which holds it, the purpose for which it was collected or the person by whom it is sought. The Committee considers that if certain parties are recognised by the community as having an exceptional, overriding and legitimate need for this type of information, these parties should first be clearly identified and then be given legal authority to access the information from particular sources. Not every government agency should be considered a potential source, as the source of information itself will convey some inference about the data subject. For example, address information from the Police might suggest criminal involvement.

#### Recommendations 3 and 4 - Control of Protected Information

The ICAC report recommends that the security of databases be constantly monitored and, where necessary, improved. This is consistent with the Committee's recommended Data Protection Principle 4 which would require that personal information be protected by reasonable security safeguards to ensure against loss or unauthorised access, use, modification or disclosure.

The ICAC report also calls for mandatory access logging procedures for "protected" information (ie. information which is not publicly available). It is unusual for data protection laws to insist on mandatory access logs. Rather, these laws normally state that recordkeepers should take whatever security measures are necessary and appropriate. Access logging is one means of improving computer security, but all it really does is help identify (corrupt) individuals who have accessed data without authority after the event. Other measures (eg. data encryption) may be necessary to stop individuals getting access to information in the first place.

#### Recommendations 5-9 - Information Protection Law

The ICAC report recommends that the State develop and implement an information protection law. Specifically, the report states that:-

- \* unauthorised dealing in protected government information be made a criminal offence;
- \* the offence provisions in the Data Protection Bill 1992 be amended in certain respects;
- \* the law should apply consistently to information held by all government departments and agencies;
- \* attempts should be made to have uniform or at least consistent information protection laws throughout the Commonwealth; and
- \* two offences should be created with respect to publicly available information, namely an offence of unauthorised release (where official release required payment of a fee) and an offence of wrongful withholding of information.

The primary aim of the suggested law is the eradication of the corrupt trade in information, rather than the protection of personal privacy. For this reason, it focuses on disclosure of information, rather than the other elements of information processing.



The exclusive focus on disclosure of information, although understandable in the context of the Report, has long been recognised by privacy and data protection practitioners as an inadequate response to misuse of personal information records. Privacy is the right of individuals to exercise some control over information which is personal to them. This control requires regulation of the whole information cycle. What information is collected and how is this done? How is it stored and processed? How is its relevance and accuracy maintained? How is it disposed of when it has served its purposes? The data protection principles developed by the Committee on the basis of well established international guidelines address all these issues.

It is also important to note that the recommendations do not suggest that the proposed information protection law apply to information held by private sector agencies. This is because the definition of corrupt conduct in the ICAC Act refers to the conduct of public officials that involves the misuse of information acquired in the course of official functions.

The failure to recommend regulation of private sector information practices is a matter for concern especially since current policies for privatising government activities have the potential to remove a large range of personal information from the scope of any regulation which applies to the government alone.

ICAC's approach may be contrasted with the Committee's recommendation that data protection legislation apply to private sector as well as public sector agencies.

Recommendation 6 concerning the Data Protection Bill suggests amendments which would strengthen Part 2 so that it reaches more corrupt conduct. If these amendments are accepted, then the Bill would link the concepts of corruption and privacy very closely. It is the Committee's view that the objects of data protection legislation should not be confused in this way. If the government wants to penalise corrupt use of information, then a simple amendment to the Crimes Act would seem more appropriate.

#### Recommendation 10 - The Private Investigation Industry

The report recommends that private investigators should continue to be licensed, and that control of the industry and responsibility for administration of the relevant legislation should be placed in the hands of Business and Consumer Affairs. In addition Codes of Conduct should be drawn up which include prohibitions on handling proscribed forms of information and obtaining information by proscribed methods. If the Code is breached, the licensee should have his or her licence suspended or revoked.

Recommendation 10 should put an end to proposals that were put forward in 1991 to abandon licensing of private investigators. If the recommendation is implemented, the Committee would be willing to participate in the framing of appropriate Codes of Conduct.

#### Recommendations 11-12 - The Principal Users of the Information

The ICAC report identified a "bridge of hypocrisy spanning the yawning gap" between the professional policies of companies concerning access to government information and the actual practices which were tolerated and even encouraged. Since the "directing minds" of companies were able to claim that they were unaware of what some of their employees were up to, the companies could escape criminal liability.

Furthermore, the Committee considered that in the absence of sufficient information to justify wide disclosure, the Committee could not endorse the disclosure of relatives interests as proposed in the draft Bill.

At the end of 1992 the Bill was yet to be enacted by State Parliament.

#### **5.11 Privacy Guidelines for HIV Testing**

In November 1992, the Privacy Committee began work on revising its 1986 guidelines on privacy and HIV testing.

The review was prompted by a request from the NSW Attorney-General's Department for the Committee to review its privacy guidelines as recommended by the NSW Anti-Discrimination Board in its *Report of the Inquiry into HIV/AIDS Discrimination (April 1992)*.

The revised guidelines will serve a two fold purpose: to describe the privacy issues which relate directly to HIV testing; and to propose a set of guidelines which will ensure that the privacy of individuals is properly considered and adequately protected.

A number of key issues will be considered within the new guidelines including HIV testing and the voluntariness of HIV tests; disclosure of test results; the uses of test results; and the testing of specific groups.

The new guidelines will incorporate the most recent medical and legal developments and will be more comprehensive in scope than the previous ones.

Consultation will be undertaken with various organisations who have expertise in HIV/AIDS policy and research. The guidelines are expected to be released in the latter half of 1993.

#### **5.12 Review of the Adoption Information Act 1990**

The *Adoption Information Act* was passed in late 1990 amid much controversy. The Act provides that adoptive children, on reaching the age of 18, may have access to original birth certificates revealing the identity of their birth parents. Access to original certificates before a child turns 18 is dependent on consent of both adoptive and birth parents.

Birth parents and adoptive parents are able to have access to certain information when the adopted child reaches 18. However, a contact register is established so that birth parents or adopted children who are about to or have reached 18 can indicate their desire not to be contacted.

The Act also provides parties to an adoption with access to a range of information held by the Department of Community services (DOCS) and various other agencies.

#### The Law Reform Commission's Review

At the time the Act was passed by Parliament, the then Minister promised a review of the Act after one year of its operation.



In addition, the Committee understood that other documents such as notices of transfer of land and valuation books (containing information as provided by the Valuer General) might also become publicly available.

In light of the scope of information to be made available, the Committee considered that all existing and proposed legislation which requires personal information to be publicly available should be reviewed to ascertain whether the social justification for making personal information publicly available outweighs privacy interests.

If there is sufficient justification for making particular records publicly available, then the framework for the disclosure of information should be established by reference to data protection principles.

#### Open Meetings

As a general rule, the draft Bill required that meetings of councils be open to the public. However, the Bill also made provision for closed meetings when certain sensitive information or matters were to be discussed.

The Committee suggested that further criteria for closed meetings be incorporated into the Bill to cover instances where the receipt or discussion of matters are deemed to be of a confidential or personal nature.

#### Sale of Personal Information

The Privacy Committee has expressed concern on many occasions at the apparent extent to which councils distribute or sell personal information. The most common sources of personal information sold include building certificates and the rate-book.

A common use of the information is for various forms of direct marketing.

The Committee recommended that the Local Government Bill incorporate provisions that expressly deal with the sale of personal information by councils.

In particular, the Committee suggested a ban on the sale of at least the following:

- \* records of approvals granted and decisions made on appeals concerning approvals;
- \* records of building certificates;
- \* the rate-book, valuation book and notices of transfer (if these documents are to be made publicly available);
- \* the roll of electors

#### Disclosure of Financial Interests

The Committee suggested that if the draft Bill does require the financial interests of spouses, de facto partners and relatives to be included on returns, this would be a significant privacy concern, particularly given the definition of the word "relative". The Committee therefore suggested that if it is considered essential to establish a publicly available register of financial interests of councillors and council officers, the information should be kept to a minimum.

The report suggests that the law relating to corporations be amended so that corporations will be criminally liable if they:

- (a) have a policy that expressly or impliedly authorises the commission of an offence;
- (b) fail to take due precautions to prevent the commission of the offence;
- (c) fail to take preventive measures once it becomes known that potentially criminal conduct has been committed on the corporation's behalf.

This recommendation could have significant implications for data protection. It would give corporations greater incentive to avoid committing offences which may be created under future data protection legislation.

The report also recommends that the Law Society of New South Wales give urgent consideration to the responsibility and obligations of solicitors with regard to their handling of confidential government information.

#### Recommendation 13 - The ICAC Act

This recommendation is not relevant to privacy and data protection issues.

#### Recommendation 14 - Bribery Law

In an earlier report ICAC recommended review and standardisation of the various bribery laws which apply in New South Wales. It renews that recommendation in this report.

The report notes that the different bribery offences under the common law, the Crimes Act, the Police Service Act and the Local Government Act are worded inconsistently and create different penalties. It recommends that these different provisions should be replaced by a "single and clear statement of the law".

In this regard, the Committee notes that if the Data Protection Bill 1992 is amended in the way suggested in Recommendation 6, then it would effectively create special bribery offences in respect of the disclosure of government information. This would not further the aim of having a "single and clear statement of the law" relating to bribery.

#### Assessment of the Report

The ICAC inquiry into the Unauthorised Release of Government Information has lifted the lid on a disgraceful state of affairs in New South Wales.

1. It exposes corrupt conduct on the part of hundreds of individuals and organisations.
2. It shows that the right to privacy, specifically information privacy, has not been adequately protected and, as a result, the privacy of many thousands of people has been infringed.

As stated previously, the recommendations made in the report are directed to the elimination of corrupt conduct, and do not pretend to be a complete answer to the privacy issues identified in the report.



Even though the focus of the report is the elimination of corruption rather than the protection of privacy, the report contains a number of strong statements in support of the right to privacy, including the following:

*"... substantial weight must be given to the right to privacy in the formulation of laws and procedures governing the handling of information. It cannot be dismissed as a mere catchcry of civil libertarians. It is an internationally recognised right" (page 177).*

*"It is difficult to see why a person's address, or any other piece of personal information, should be more or less readily available to those who claim to be the person's creditors, or to the public generally, because of the government department which happens to hold it. The decision should not rest with the department. It does not own the information. If the information is "owned" at all, it belongs to the person to whom it relates. If it has been made available to a government department for a specific purpose, then in the absence of special circumstances, that department should not use it, or allow its use, for any other purpose" (page 153).*

*"It is not just the nature of the information, or the fact that people may know it, that is important. What is basic to the right is control over personal information" (page 187).*

The ICAC report on the Unauthorised Release of Government Information should be the catalyst for major legislative changes in New South Wales, including the enactment of a comprehensive data protection law.

The Privacy Committee has been waiting for 10 years for the Government to enact such legislation - surely the Committee, and the people of New South Wales will not be made to wait much longer.

#### 4.2 Data Protection Bill 1992

As reported in last year's annual report, the Data Protection Bill 1991 was introduced into the New South Wales Parliament as a Private Member's Bill. This Bill was re-introduced in 1992 and debate was expected to be deferred until the Independent Commission Against Corruption (ICAC) reported on its inquiry into the Unauthorised Release of Government Information.

On 12 August 1992, the day that ICAC released its report, the Attorney General, Mr. Hannaforde announced that his Department would prepare the necessary privacy legislation to overcome the obvious infringement of privacy and other problems identified in the report.

The Committee took the opportunity to draw the Attorney's attention to the proposals for legislation set out in its report entitled *"Privacy and Data Protection Legislation in New South Wales - A Proposal for Legislation"* (Report No.63, June 1991). The Committee also offered to provide whatever further assistance was required to draft the legislation.

The Committee was assured that it would be consulted in the refinement of the legislation to ensure that the legislation adequately protects privacy rights, and in particular information privacy rights.

Consultation with the Department continued throughout the remainder of 1992. In a speech made on behalf of the Attorney General in December 1992, Mr.

The Committee also wished to be informed of any requirements for the hospital operator to ensure security and confidentiality of records and to prevent unauthorised secondary uses, as well as any procedures for ensuring appropriate disposal of records once they are no longer required for patient care or administrative purposes.

In December 1992, the Department responded that it would acquire ownership of the existing records, but the physical transfer of the records would take place in much the same fashion as would be the case if a private medical practice changed hands. However, individuals wishing their records to remain under the control of the Department would be able to do so, although they would be asked to acknowledge their full responsibility for any clinical disadvantage that might accrue from this choice.

At the end of the reporting period the Committee was still in the process of assessing the Department's policy with respect to the transfer of records. The Committee will provide further comment in order to respond to any complaints arising in 1993.

#### 5.10 Draft Local Government Bill 1992

Local government maintains many records which contain personal information about citizens of New South Wales. This information is usually held by local councils and includes the names and addresses of residents and ratepayers, information about rates due or payable, pensioner status, building certificate applications, land use and even dog ownership. Further detailed information is also recorded in relation to relevant interests of councillors and designated employees.

On 20 December 1991 the Minister for Local Government in New South Wales released an Exposure Draft of the *Local Government Bill 1992*.

In commenting upon the Bill, the Committee's primary concerns related to the handling of personal information about individuals. The Privacy Committee believes that councils, like other recordkeepers, should comply with data protection principles in the collection, storage, use and disclosure of personal information.

##### Publicly Available Information

The most important data protection issues raised by the Exposure Draft Bill relate to the various categories of personal information which are, or may become, publicly available. This information includes:

- \* personal information disclosed at meetings of the council and reports tabled at, or submitted to, meetings, and;
- \* personal information contained in documents made publicly available under Clause 14 of the Exposure Draft (*Access to Information: What information is publicly available*). Documents in this category include returns of councillors' interests; returns as to candidates campaign donations; agendas for council and committee meetings; minutes of council and committee meetings; records of approvals granted and decisions made on appeals concerning approvals; and records of building certificates



In August 1992 the Privacy Committee made a submission to the Standing Committee.

The Committee's submission focused on a number of issues surrounding the exchange of LEAN data, emphasising the fact that the Committee was not satisfied that the advantages of LEAN would outweigh the disadvantages or potentially serious breaches of privacy which could occur. The Committee also raised concerns about a number of technical aspects of the network.

Throughout the latter part of 1992, the Privacy Committee also gave advice to the NSW Attorney General's Department with respect to the privacy implications of LEAN.

Some of the matters that continue to concern the Committee are:

- \* the absence of protection against an extension of LEAN;
- \* the absence of clear legal definitions of law enforcement and revenue protection uses;
- \* the absence of clear and adequate proposals to publicise the operation of the scheme and the rights and interests of data subjects; and
- \* the need to ensure that adequate safeguards apply when New South Wales information is accessed and shared by users in other states.

The Committee sees the resolution of these issues to be of prime importance if LEAN is to be implemented. The Committee continues to monitor the development of LEAN.

## 5.9 Privatisation of Public Hospital

The Privacy Committee received a number of complaints about the proposed transfer of medical records from the public hospital system to a private operator. This arose from a recent State Government decision to close the Hastings District Hospital and replace it with a privately operated hospital at Port Macquarie.

The contract for the proposed transfer contained a provision for patient records currently in the custody of a public hospital to be released to the private hospital's new operator.

In view of the sensitivity and confidentiality of such records, and the right of access which patients currently enjoy under Freedom of Information legislation, the proposed transfer raised significant privacy issues.

The Committee wrote to the Director-General of Health seeking clarification of a number of issues including, the legal basis for transferring such records, the continuing departmental responsibilities in relation to patient access under FOI, and any proposals to notify the proposed transfer to the patients concerned and to obtain their consent.

Andrew Tink, M.P., announced that the close consultation with the Privacy Committee would result in a legislative proposal which reflects very closely the recommendations made by the Committee in its June 1991 report. Specifically under consideration for inclusion in the Bill were:

- \* prohibition of a public employee or former public employee from using, disclosing or offering any personal information to which the employee has had access in the performance of his or her official functions;
- \* establishment of the position of Privacy Commissioner;
- \* provision for each Department Head and each Chief Executive Officer of an Authority of the State to prepare a policy for the Department or Authority to comply with the Data Protection Principles within 12 months of the commencement of the legislation;
- \* provision for each Department's or Authority's data protection policy to be approved by the Privacy Commissioner;
- \* the functions of the Privacy Commissioner to relate immediately to the public sector, but to only relate to the private sector to the extent to which the private sector is eventually covered by the proposed legislation by way of Codes of Practice. However, it could be open to the Commissioner to investigate complaints concerning the private sector as the Privacy Committee does now, to promote privacy and conduct research into privacy matters pertaining to the private sector;
- \* provision for regularly reviewable exemptions from the operation of the legislation for areas or types of information and activity but not in relation to access to, or correction of, personal information by the subject of that personal information; and
- \* provision for "public registers" to be limited to those listed in a schedule to the legislation and for the following principles to be applied in relation to access to data on those registers:
  - (a) the re-use of data in public registers should be limited to purposes which are compatible with the purpose of collection;
  - (b) there should be a mechanism for the suppression of information about individuals whose safety or privacy would be particularly threatened if listed in a public register;
  - (c) data subjects should be advised of the purpose and public interest in the maintenance of the register.
- \* provision for the Privacy Commissioner, at the request of a private sector group, or at the request of the Minister, or of his or her own motion, to prepare or review a Code of Practice relating to personal information held by that group.

Consultation with the Attorney General's Department is expected to continue in 1993.



#### 4.3 Computerised Operational Policing System (COPS)

There are many circumstances in which police are expected to have ready access to information in order to carry out law enforcement tasks. While the efficient storage and retrieval of information is vital to the effectiveness of police operations, a balance must be achieved between access to information and the protection of individual rights to privacy.

Throughout the year the Privacy Committee was involved in providing comments and advice on the development of the New South Wales Police Service's Computerised Operational Policing System (COPS). COPS involves a systematic review and restructuring of all existing police computerised information resources. These are currently stored in a number of separate systems which have been criticised as being diffuse and difficult to access. COPS uses information engineering techniques to standardise and connect the various kinds of information held, so they can be flexibly presented on a series of menu driven screens in answer to queries from any officer with access to the system.

This will occur in three stages. Stage 1 is due to commence in 1994 and will record all incident and criminal intelligence data, and provide management reporting capabilities. Once this is established, on-line charging, warrants and criminal records will be added in stage 2, and advanced communication and imaging technology is expected to be added in stage 3.

The Committee is concerned that the wide availability of, and access to, personal information on the COPS system will have a significant potential for misuse and widespread intrusion into personal privacy.

The general policy endorsed by the Committee is that where information is collected for one purpose it should not be used for another without the consent of the data subject or the authority of law. While there is a public interest in the police having access to information where there is a need to investigate particular offences, if powerful computer systems like COPS are established they need to incorporate design features to ensure that they are used in an appropriate and responsible way. There also need to be clear policies controlling the behaviour of users, and providing accountability standards which can be independently audited.

The issues of data linkage and data access are the most critical from a privacy perspective. When the full range of information collected for a variety of police purposes is combined on COPS there is a danger that routine access to it will represent an unfair and unacceptable level of surveillance.

The fact that so much information will be able to be assembled about a person also raises concerns about peoples' access and correction rights, and about disposal of information which is no longer reliable or relevant.

These complaints raised the general issue of the way in which subpoenaed documents containing personal information are handled **after their presentation** in court.

Two cases in particular were cited. One of these related to a matter before the Supreme Court of NSW in 1986. It was alleged that two departmental files subject to subpoena were returned to the Department in February 1992 by a person who had acted as solicitor for the plaintiff, and who claimed that they had been given to him by the court at the end of the proceedings. The files contained personal information about a number of individuals.

The other relates to a matter brought before the District Court in Sydney in 1991. In this case the file returned by the court was found to contain photocopies of the plaintiff's medical record which were not part of the departmental file.

The Committee raised these matters with the NSW Department of Courts Administration which is responsible for the operation of the court registries. The Department then sought advice from the Deputy Chief Executive Officer of the Supreme Court of NSW and the Principal Courts Administrator of the District Court of NSW as to rules and procedures surrounding the handling of subpoenaed documents.

Despite each court handling a large number of documents every day, the Department of Courts Administration was confident that proper procedures were in place for the correct handling and return of documents and that these were followed by registry staff. However, the Department also suggested that both courts are often faced with circumstances in which they have no control over the flow of documents. It was also suggested that the problem might lie with legal practitioners who are given access to documents produced on subpoena.

The Committee was satisfied that the Department of Courts Administration had sufficiently drawn the attention of both courts to the issue of privacy protection in the handling of subpoenaed documents. Subsequent approaches were also made to the Law Society and the Bar Council drawing attention to the responsibilities of practitioners.

#### 5.8 Law Enforcement Access Network

The past two Annual Reports have referred to the Privacy Committee's concerns about the proposed Law Enforcement Access Network (LEAN).

The LEAN proposal would involve the combining of data from a number of New South Wales agencies including the Land Titles Office, the Water Board and the Valuer General's Office. This information would be networked with land data from other states and with companies information from the Australian Securities Commission. LEAN could then be accessed by State and Commonwealth government agencies for the purpose of revenue protection and law enforcement.

The LEAN proposal would allow sophisticated computer power to be harnessed for data searching and matching using a wide number of fields.

As part of the Federal government's assessment of LEAN and other measures for controlling fraud against the Commonwealth, the House of Representatives Committee of Inquiry into Fraud examined the LEAN proposal.



Whilst not a common problem, Munchausen's Syndrome by Proxy is a complex condition which is difficult to diagnose and manage. Hospital staff may need to establish whether they are dealing with a case of the syndrome when a child is admitted to hospital and the parent suspected of having the condition is constantly with the child. For obvious reasons, the hospital will not wish to make the diagnosis without convincing evidence.

The use of video surveillance is proposed as one option where other forms of monitoring have failed to document the syndrome. In view of the exceptional nature of the illness, consent of the parent would not be sought.

The Committee was prepared to accept that, in balancing a hospital's duty for the care and treatment of children against the interests of patient and parent privacy, the use of video surveillance could be justified provided there were proper safeguards in place. Tapes should not be retained unless they are needed for further action. Non-identifying information on the incidence of monitoring should be publicly reported to establish a minimum level of public accountability.

The Committee was concerned to ensure that any surveillance should be directed primarily to patient care rather than legal intervention. The potential conflict between the hospital's role as a provider of care in circumstances of confidentiality and the law enforcement consequences of detecting behaviour through the use of video cameras should be clearly addressed in procedures relating to the authorisation of surveillance and the use of videotapes. Safeguards against unfair use of surveillance should include access by parents or their legal advisers to potentially incriminating tapes and inclusion of a representative of the Legal Aid Commission or Community Legal sector on the committee set up to authorise video monitoring.

The Committee suggested that there was a danger that video surveillance could be adopted as a cheaper alternative to more thorough and careful investigation. Given the relative rarity of the syndrome, it needs to be asked whether permanent facilities for routine monitoring are justified. The existence of a permanent monitoring facility may also encourage its use for other forms of surveillance where the justifications applicable to Munchausen's Syndrome by Proxy are not as strong.

Doubts were expressed as to whether the use of video monitoring would remain confidential. It is likely that a parent who is the subject of surveillance will eventually discover this fact from staff who are aware that cameras are installed. The uncontrolled way in which this happens may heighten the breach of privacy involved and complicate further treatment.

The Committee's response to the draft guidelines underline the need for a balanced overview of all aspects of similar video surveillance proposals.

#### 5.7 Privacy and the Handling of Subpoena Documents

The Privacy Committee was asked by a federal government department to investigate complaints which had arisen in relation to the custody and return of subpoenaed documents in civil actions.

In the early stages of development of COPS, the Committee wrote to the Police Commissioner stating that it would be pleased to provide privacy policy advice to the project team. Following a positive response from the Commissioner, Committee staff were extensively briefed on the development of the project, and were able to make a number of suggestions on privacy aspects. The Committee was subsequently invited by the Police Privacy Focus Group to discuss privacy and data protection policies which would accompany the introduction of COPS. It remains to be seen whether the Committee's concerns can be accommodated within the design of the system and associated policies.

Despite a suggestion in September 1992 by the then Minister the Hon. E.P. Pickering MP that the COPS project had been put on hold, authorisation for the resumption of the program was confirmed by the new minister, the Hon. Terry Griffiths MP, in December. The Committee is continuing to monitor the development of COPS.

#### 4.4 Health Communications Network

Improvements in communications technology have made a great impact on health care and medicine. While the need for sensitivity and security in dealing with patient information is of paramount importance, an improved health information flow may significantly benefit both the community and the health care profession.

In September 1991 the Australian Health Ministers' Conference (AHMC) agreed to establish a joint Commonwealth/State Working Group to look at the long-term information needs of the health care system. A workshop convened by the Working Group was conducted in December, 1991.

The Report of the workshop identified a number of flows in current health information systems, including significant blockages to information flows, lack of a coherent overall plan or vision of where health information was heading, and significant legal, ethical and standards issues requiring timely resolution.

In April, 1992 a meeting of AHMC considered a report of the Working Group. The report listed a number of advantages to be gained from a planned and co-ordinated national response based on a health communications network linking hospitals and individual practitioners.

Consultants were then briefed and the Committee understands that an Interim Business Case and Implementation Plan has been presented to the AHMC.

Applications for pilot projects to test the feasibility of the scheme were sought in late 1992 and it was expected that about ten pilot studies would commence in early 1993.

Some of the advantages of a health communications network have been said to include quicker access to patient care information, provision of access in rural or remote areas, facilitation of access to international medical expertise and international access to organ donor lists.



Proponents of the Health Communications Network have stressed that this is not a proposal for a "central database" but rather that health information will continue to be stored in a decentralised manner. It is acknowledged, however, that the network is intended to involve a high level of standardisation and there is likely to be some pressure on institutions and practitioners to participate. Indeed the Australian Doctors Fund has expressed particular concerns about these pressures.

Currently the proposal appears to anticipate that private firms will be able to implement the network on existing telecommunications networks with State and Commonwealth health departments sponsoring the development costs and individual users paying the cost of accessing the system.

As the network is still in the developmental phase, and the Committee has not seen any firm proposals for its operation and structure, it appears that information storage will remain with individual practitioners and institutions, rather than being accessed from a centralised computer. If this is the case, the conditions under which users will have the right to access information from other sources or the obligation to supply the information held by them will be crucial to how confidentiality and data protection issues and guidelines can be addressed.

Concerns might also be raised about the law enforcement implications of such a large communications network of health information. Law enforcement agencies may well be tempted to access such a network for the purpose of assisting their investigations. Accordingly, safeguards would have to be built into the system in order to deter misuse.

The Committee continues to monitor progress in the development of the Health Communications Network, with specific reference to the proposed means for protecting the privacy of patient information as a priority.

The Committee will also continue to encourage the process of broad public discussion of the privacy issues raised by this proposal.

#### 4.5 Drug Testing in the Workplace

The Committee first highlighted its concerns about workplace drug testing in a 1988 Privacy Bulletin. In this publication the Committee noted that, given the privacy invasive nature of drug testing, very strong arguments would be required to justify any workplace drug testing program.

In New South Wales workplace drug testing is already carried out on the roads, on the railways, by some airlines and by mining companies. Drug testing of professional sports people is also performed.

The extent to which workplace drug testing was being used in other contexts was not clear, but in 1992 there were indications that many employers and some industry regulators were considering whether to introduce drug testing.

The Committee decided that a comprehensive review of the privacy implications of workplace drug testing was necessary, to ensure that the privacy issues associated with workplace drug testing received the fullest consideration by employers, industry regulators, government and the community at large.

With respect to the reform of registry procedures, the Committee maintained its 1989 position that the Registrar should be required to formulate regulations which will govern procedures for access to the Registry and that regulations should include a list of agencies "authorised" to have direct access to Register information and a statement of the purposes as to why access should be permitted. The Committee also suggested that it should be given the opportunity to comment upon any such proposed regulations.

#### Access to Certificate Information

On the basis of data protection principles, the Committee opposed unrestricted access to birth and marriage certificate information. So far as death certificates are concerned, some argue that the dead have no right of privacy. The Committee noted, however that death certificates contain significantly more information than the death index and include information about the deceased's next-of-kin, former spouses, and children. Death certificates also reveal where a person died and the cause of his or her death. This information may be capable of causing embarrassment to the person's family. For example, the place of death may be in a prison, a drug clinic, a psychiatric hospital, or a brothel. The cause of death may be suicide, AIDS or even an inheritable condition. The Committee therefore opposed open access to all death information.

#### Access to Indexes

With respect to information contained on the indexes, the Committee also adhered to its 1989 position that if feasible, information entered into the Birth Index should only be made public after the subject has died. If not feasible, the information entered should only be made public after 100 years.

With respect to the marriage index, the Committee suggested that this should only be open after 85 years.

The Committee also recommended that public access to the death index should be made available.

At the end of 1992 the Standing Committee was preparing its report to the New South Wales Parliament.

#### 5.6 Video Surveillance to detect Munchausen's Syndrome by Proxy

Video surveillance is increasingly being turned to as an inexpensive means of resolving security problems. There is a need to carefully consider the social implications of what is often seen as a purely technical solution. The delicate problems which this technology can raise is illustrated by advice given by the Committee to the New South Wales Health Department on draft guidelines for the surveillance of suspected victims of Munchausen's Syndrome By Proxy.

Munchausen's Syndrome by Proxy is a relatively rare syndrome in which an adult, often a parent, invents stories of illness in a child in order to seek attention and medical care for the child. This may involve fabricating symptoms by injuring or poisoning the child, sometimes leading to the child's death. In these circumstances the behaviour can lead to serious criminal charges.



### Functions of the Registry

The LRC Report noted that (at page 1):

*There is little legislative guidance for the performance of the diverse and often vaguely defined functions expected of the Principal Registrar. His statutory powers are expressed in very wide terms. Some functions of the Registry have developed outside the legislative framework, relying on regulations and administrative processes to fulfil the demands of government. This has occurred without an independent review of the role of the Registry.*

The Committee considered that from a data protection viewpoint, the fact that the appropriate purposes of the Register are undefined is totally unacceptable. The Committee's data protection principles require that the purposes of collection of births, deaths and marriages information should be specified before information is collected.

Once purposes to be served by the Register have been clarified, the rules governing access to Register information can and should be prescribed by law, thus restricting the exercise of administrative discretion.

In the meantime, the Committee recommended no change should be made to the existing procedures for access.

### Difficulties with a "Closed Register"

The LRC Report argued that since the effective operation of a 'closed' system cannot be guaranteed, an open register system should be substituted.

The Committee considered this reasoning to be completely erroneous. Data protection laws operate on the basis that, in general, registers of personal information should be closed and access to the information without the consent of the subjects should be restricted by law to specific socially justifiable purposes. If the existing procedures for restricting access lack certainty and do not comply with the data protection principles then these procedures require reform.

The Committee was also wary of the argument that open access should rely entirely on the discretion of the Principal Registrar. The Committee suggested that reliance on the discretion of the Registrar is not an adequate means of restricting access to births, deaths and marriages information. The Committee argues that the solution to increased access relies not in an open register, but in specific application of data protection rules governing the collection, handling, use and disclosure of the information. Appropriate data protection rules will serve to eliminate arbitrary decisions in relation to access by eliminating or greatly restricting the area within which the Registrar can exercise discretionary powers.

### Access to Registry Information

The Committee concluded that the current procedures for access to Registry information do not conform with the data protection principles and therefore require reform. The Committee opposed the LRC's recommendation that the registry should become an open one.

In October 1992 the Committee published a report entitled Drug Testing in the Workplace, the major findings of which are set out below.

### The Privacy Issues

The privacy issues raised by drug testing in the workplace relate to both physical privacy and information privacy.

Physical privacy can be described as the interest people have in maintaining a degree of freedom from interference with their person and their personal space. Drug testing is invasive of physical privacy, particularly because urine testing (one of the most common forms of testing for drugs other than alcohol) involves close observation of urination in order to prevent cheating.

Information privacy can be described as the interest people have in exercising some degree of control over the collection, storage, use and disclosure of information about themselves. The Committee is particularly concerned to ensure that workplace drug testing programs are carried out with full reference to the Committee's data protection principles including principles about the fair and lawful collection of information, informed consent, data quality and security, and proper use and disclosure of personal information.

### Limitations of Drug Testing

The Committee's research into drug testing revealed that current technologies suffered from problems relating to the accuracy and relevance of test results and the cost of testing. These limitations can be expected to restrict the usefulness of drug testing in many contexts.

There are doubts about the accuracy of drug testing by laboratories other than those accredited to do medico-legal work. In particular, it is well established that immunoassay tests, the most commonly used technique, can lead to a significant number of false positives. False positives are test results which indicate that a given drug is present when that drug is actually absent in a sample of urine (or is present in concentrations below the designated cut-off level). Immunoassay drug testing can also result in people apparently testing positive to prohibited drugs, when they have in fact taken common non-prescription medicines such as cough mixtures or cold and flu remedies.

Whatever laboratory technique is used, the drug testing process is vulnerable to human error in the handling and testing of samples. The possibility of contamination or misidentification could have serious consequences for the person being tested.

Given the expensive nature of the drug testing process, employers may be tempted to use cheaper techniques which are less accurate. Employers should always use the most accurate methods of workplace drug testing and must not be tempted to compromise on cost. Workplace drug testing should only be carried out by accredited laboratories who are certified to conduct tests to accepted medico-legal standards. Legal requirements are needed to ensure that this is the case.

Another problem is that it is not practical for an employer to test for all drugs that might cause impairment, or even to test for all illegal drugs because of the costs and the inherent limits of currently available analytical techniques. There are also too many illegal drugs in the marketplace to warrant testing for all of them.



Impairment

Perhaps the most fundamental limitation of drug testing is that most current forms of drug testing cannot measure whether a person's work performance is actually impaired by the drug that has been detected. Nor is it possible to detect when the person used the drug.

Except in the case of alcohol breath testing, all that can generally be concluded is that the person testing positive has been exposed to the drug in some way or other, whether deliberately or inadvertently.

The limitations of relating drug test results to degree of impairment severely restricts its usefulness in safety related contexts. As urine testing cannot show impairment, it is hard to see how the testing of existing or potential employees will significantly improve safety or productivity at work.

Are There Alternatives to Drug Testing?

The Privacy Committee found that there are alternative, less privacy invasive means of addressing workplace problems caused by the use of alcohol and other drugs. Drug testing is clearly not the only way in which these workplace problems can be addressed.

Given the problems associated with drug testing, these alternatives should be preferred, or at least tried, before a drug testing program is considered and implemented.

Alternative approaches focus on workplace education, on the safety and health implications of drug and alcohol abuse, and the training of supervisors and managers. Managers and supervisors can be trained to recognise performance indicators which suggest that an employee has an underlying problem possibly involving drugs, and arrange the referral of the employee for further assistance.

Is Workplace Drug Testing Justified?

Proponents of drug testing advance a number of justifications for the use of drug testing in the workplace. These include concerns about workplace safety, productivity, employee health, and concerns about the integrity and honesty of employees.

Of the possible justifications for drug testing the Privacy Committee concluded that workplace safety is the only concern of such importance that, in limited circumstances, it could justify testing.

Many jobs can pose a safety risk if the people involved are impaired by drugs. However, with the exception of alcohol breath and blood testing, it seems that drug testing can do little to alleviate safety concerns, unless it is deemed that any detectable level of certain substances is unacceptable.

The Committee's Recommendations

In light of its investigation the Committee made three recommendations with respect to the use and control of workplace drug testing.

that the community has a poor understanding of mental illness. There is a mistaken view that mental illness makes a person dangerous. Consequently, many mentally ill, but harmless people may be reported, but the genuinely dangerous, yet mentally healthy individuals will not be reported. Reporting may even deter some mentally ill people from seeking treatment for fear of a report being made to police.

The Committee also raised the issue of the accuracy and timeliness of reports about allegedly dangerous people. Even if a report was completely accurate at the time it was made, it could become quickly out of date and inaccurate. A person may be dangerous for a short, acutely stressful period and thereafter present no threat to the community.

Overall, the Privacy Committee concluded that the proposal could lead to the collection of information of dubious quality and doubtful probative value. The Committee advised the Attorney General's Department that the reporting scheme would amount to an unjustified invasion of the privacy of people who are reported.

**5.5 Inquiry Into An Open Births, Deaths and Marriages Registry**

The Registry of Births, Deaths and Marriages collects, maintains and controls a range of sensitive personal information about people in New South Wales. Some examples include date of birth, place of birth, name of mother, name of father, religion, occupation, date of death, cause of death etc.

Information held by the Registry has never been freely available- the public has an expectation that information which is compulsorily supplied to the Registry will be kept confidential. Only those whom the Registrar deems to have a 'sufficient interest' are permitted access to certificate information.

In 1989, the New South Wales Law Reform Commission released its report entitled "Names: Registration and Certification of Births and Deaths" (the LRC Report)

Recommendation 1 of the LRC Report stated that:

*The register of Births, Deaths and Marriages should become an open register available to all members of the public, except for those parts which are closed by statutory authority*

The Committee's 1989 submission on the LRC report opposed an "open" registry system in favour of the Registry's existing system of restriction of access (details of the Committee's policy are set out in its 1989 Annual Report).

In 1992 the Committee was invited to make a submission to the New South Wales Legislative Council's Standing Committee on Social Issues Inquiry into an Open Register of Births, Deaths and Marriages.

The Committee's 1992 submission continued to oppose an open register on the same grounds as outlined in its earlier submission. The 1992 submission also made a number of additional comments on the issue of an open register.



#### 5.4 Joint Select Committee on Gun Law Reform

A Joint Select Committee on Gun Law Reform was set up by the New South Wales Parliament in the wake of a mass shooting incident in the Sydney suburb of Strathfield. Its purpose was to inquire into ways of providing tighter controls on the ownership and availability of firearms.

The key recommendations made by the Select Committee were that:

- 2.1 *[The] Government should develop procedures, having regard to privacy issues, for the voluntary reporting to police by any person, and in particular, health professionals and community workers, of those people who would be likely to be dangerous to themselves and/or others if they have access to, or continue to have access, to firearms*
- 2.2 *The New South Wales Police Service [should] introduce a formal system to follow up voluntary reports referred to in 2.1 and, following an investigation, if the person possesses firearms, police should remove the firearms pursuant to Section 35 of the Firearms Act 1989*

The Privacy Committee was asked by the NSW Attorney General's Department for comment on these and other recommendations made by the Joint Select Committee.

The Privacy Committee was concerned that the recommendations of the Joint Select Committee's report may give rise to the establishment of a "dangerous persons" database. The database would involve a system of reporting to police persons who, in the opinion of others, would be likely to be dangerous with firearms.

In commenting on the Joint Select Committee's report, the Privacy Committee made specific reference to data protection principles. The Committee was concerned that breaches of the data protection principles may occur because, among other things, information could be collected without a person's knowledge which was irrelevant, inaccurate or unduly privacy invasive.

The reporting proposal anticipated that the police would receive reports about people likely to be dangerous if they had access to firearms, from any person willing to make one. Those reported would not necessarily be made aware of the report, or of the reason why they were reported.

The Committee pointed out that information which alleges that a person is dangerous will not be relevant if the person does not have a firearm, does not have access to a firearm, and never intends to obtain one. Furthermore, it is difficult to judge whether a person should be considered "dangerous". The Joint Select Committee report suggested that people who are mentally ill should be reported. However, there are many other circumstances in which people who do not suffer mental illness could present a danger (for example, jealous, angry or abused people) and therefore be reported.

Clearly, what constitutes a "dangerous" person would be a matter of subjective judgment, a judgment that even trained psychiatrists could find difficult, and which is clearly beyond the capacity of the ordinary person. Another problem is

The first is that workplace drug testing, other than that specifically authorised by legislation, should only take place when:

- (a) a person's impairment by drugs would pose a substantial and demonstrable safety risk to that person or to other people,
- (b) there is reasonable cause to believe that the person to be tested may be impaired by drugs, and
- (c) the form of drug testing to be used is capable of identifying the presence of a drug at concentrations which may be capable of causing the impairment.

The Committee also recommended that workplace drug testing should be prohibited by legislation other than in the circumstances stated in the first recommendation.

Finally, the Committee recommended that workplace drug testing which is permitted should be subject to procedural standards, set out in legislation, to protect the privacy interests of those who are tested. No work place drug testing program should be implemented before procedures are clearly established for:

- \* Sample collection including procedures which preserve privacy to the maximum extent possible.
- \* Chain of custody procedures to prevent accidental loss, misidentification or tampering with or exchange of samples.
- \* Threshold concentrations for each drug which will determine whether a test result can be considered "positive".
- \* The storage and security of personal information collected through the drug testing program.
- \* The use and disclosure of personal information collected through the drug testing program.
- \* Permitting the individuals tested to obtain access to personal information relating to their drug test, including the result and the conclusions, if any, drawn from the test and to seek correction of this information through repeat testing of the sample.

Organisations that undertake drug testing should have formal written policies to inform people about these procedures and in particular to enable them to easily ascertain:

- \* the circumstances in which they may be tested;
- \* the purpose of testing;
- \* the drugs that will be tested for; and
- \* the various possible consequences of a drug test result.



A Comment on Drugs in Sport

The Committee's report also contained comments on drug testing in sport.

A number of justifications have been put forward with regard to drug testing in sport. The most prominent ones relate to the use of drug testing to ensure fair play and the integrity and honesty of participants in sport. The protection of competitors' health and safety, and the issue of impaired performance have also been put forward as important justifications.

With respect to the issue of impaired performance, some sports organisations have taken the view that they are justified in testing for drugs such as alcohol and cannabis.

Testing for cannabis on the basis that it may impair performance is not justified. Players can and should be judged on their performance in training and on the field in competition. There is no need to test biological samples. In any case, as was noted above, drug testing is not a reliable indicator of current impairment.

The Committee concluded that it did not oppose drug testing in sport which is authorised by legislation. Testing for performance enhancing drugs has legislative recognition and has been accepted by competitors and the wider community as being necessary to fair play in sport.

However, sports competitors should not otherwise be required to submit to drug testing except for safety reasons.

The Committee made the following recommendation:

Drug testing in sport, other than specifically authorised by legislation, is only justified when:

- (i) a person's impairment by drugs would pose a substantial safety risk to that person or to other people; and
- (ii) there is reasonable cause to believe that the person to be tested may be impaired by drugs; and
- (iii) the form of drug testing to be used is capable of identifying the presence of a drug at concentrations which may be capable of causing impairment.

#### 4.6 AUSTEL Inquiry into the Privacy Implications of Telecommunications Services

New telecommunications technologies bring with them the promise of greater efficiencies in the cost and quality of services, but they also have implications for privacy that must be anticipated and given proper consideration.

In October 1991, the Australian Telecommunications Authority (AUSTEL) announced an inquiry into the privacy implications of some telecommunications services both currently available and planned. The terms of reference highlighted caller ID, automatic calling equipment, traffic management systems and telemarketing as particular services which have privacy implications.

Assessment of health risk would take into account the time an individual is likely to be held in custody prior to further assessment and the potential risk to the safety of the person whilst the person is in custody.

The Privacy Committee was invited to comment on the Report and recommendations. Having assessed the privacy implications of the Inter-Departmental Committee's proposed system of information exchange, the Committee wrote to participating agencies seeking further advice about a number of issues including:

- \* the methods of recording, storing and handling information made available to the department;
- \* the procedures for classifying appropriate levels of access to different classes of information;
- \* the measures proposed or currently established to ensure security for confidential health information;
- \* the consequences of the proposed transfer of information for existing procedures for obtaining prisoner consent to access medical records;
- \* the procedures for enabling prisoners to access health information relating to themselves and to correct inaccurate information; and
- \* procedures for disposing of such material once it was no longer relevant to custodial requirements.

Custody and Privacy Erosion

One of the primary concerns of the Committee is that the proposal to collect and transfer health related data on *all* prisoners may well lead to the identification of a minority of people at risk at the expense of a significant erosion of privacy and confidentiality amongst the prison population as a whole. Consequently, questions arise as to whether the Inter-Governmental Committee's proposal is the most privacy sensitive means of minimising risks to the health and safety of people being held in custody.

The Committee is also concerned to ensure that the exchange of health related information between Departments is consistent with the Committee's data protection principles. The issue of consent is one which the Committee will monitor as the Inter-Departmental Committee provides further detail about the specific nature of the information sharing arrangements.

At the end of 1992 the Privacy committee met with members of the Department of Corrective Services and Inter-Departmental Committee to discuss the initial Report.

The Committee will continue to liaise with the Inter-Departmental Committee with respect to the resolution of issues associated with the development and implementation of appropriate health information sharing guidelines.



Data protection principles also require that personal information should be solicited, wherever possible, directly from the individual concerned. The form asked the applicants to provide medical details about their family members. The Committee advised that information on family members should not be obtained without the knowledge and consent of the family members concerned.

The company claimed that another purpose served by the health assessment forms was to collect information to help employees with medical and occupational health advice during the course of their employment. Collection of personal information for this purpose is likely to be inappropriate in a pre-employment context, because information may be collected unnecessarily on people other than the eventually successful applicant.

The Committee recommended that if the company wished to collect a comprehensive medical history in order to offer health related assistance, then employees should be informed of this purpose and asked to voluntarily provide information if they wish to participate.

More generally, the Committee noted that alternative approaches to pre-employment health assessment have been developed which do not require excessive collection of personal information and which are therefore more consistent with the data protection principles.

One such approach analyses the job demands of the different job classifications within an organisation, for example, professional, clerical, technical. This allows the scope of health questionnaires and subsequent medical testing to be limited to what is necessary for the job being applied for. Instead of collecting information from job applicants about the presence of specific medical problems, questionnaires should be made to focus on the issue of fitness to carry out the work required.

### 5.3 Exchange of Health Related Information on Persons in Custody

In March 1991 the Custody Health Inter-Departmental Committee was set up in New South Wales to ascertain the most effective way of reducing both Aboriginal and non-Aboriginal deaths in custody.

The risks of deaths in custody and the need for more efficient exchange of health and other information about persons at risk within the prison system and in police custody were highlighted in the *National Report of the Royal Commission into Aboriginal Deaths in Custody* (May 1991).

In July 1992, the Inter-Departmental Committee's Chairman wrote to the Privacy Committee seeking advice on its initial Report which contained guidelines on the assessment and recognition of vulnerable persons. The Inter-Departmental Committee had determined a minimal level of information about persons in custody which should be communicated between departments and services so as to ensure the safety of persons at risk.

The sort of information to be collected and exchanged includes information about past and present medical problems (including psychiatric), drug and alcohol problems, personal and social adaptation and the prisoner's behaviour and attitude to imprisonment.

In February 1992, the Privacy committee made a submission to the AUSTEL inquiry.

### Privacy and Telecommunications

Some uses of telecommunications services raise privacy issues related to "intrusion". For example, unwanted telephone calls or facsimile transmissions may invade privacy by forcing themselves on the attention of the recipient. The use of automatic calling equipment may add to the potential for telecommunications based intrusions.

The provision of telecommunications services also results in the collection of a great deal of data about the users of these services. For example, billing data may be collected containing the telephone number and address of telephone subscribers along with the number of units to be charged, the called telephone numbers, the type and duration of calls and the volume of data transmitted. Traffic data may also be collected containing personal information necessary to establish calls, such as telephone numbers, and other details of services used by a subscriber.

In its submission the Committee concluded that telecommunications services raise a number of important privacy concerns relating to data protection and to intrusions on personal privacy. The Committee also recommended that the telecommunications industry should seek to comply with general data protection principles in the processing of personal information. These principles are set out in the Committee's 1991 report on *Privacy and Data Protection in New South Wales*.

### Caller ID

AUSTEL highlighted Caller ID, sometimes referred to as Called Number Display, as one service which raises significant privacy issues. Caller ID permits the display of the number from which an incoming telephone call originates. This information may be displayed on a screen connected to the receiving telephone. From the telephone number it may be possible to deduce the identity of the caller even before answering the call, either because the called party knows the telephone number or through the use of number-to-name databases.

While phone companies have highlighted the benefits this provides to individuals, Caller ID can be used as a covert means of collecting personal information. For example, a business could collect the phone numbers of all people who make enquiries about its products or services. Using a reverse telephone directory it would then be possible to match a telephone number with names and to use this information for direct marketing purposes.

Caller ID has important implications for information privacy. Information privacy is the interest people have in controlling when and to whom they reveal information about themselves. To the extent that Caller ID takes this prerogative away the facility lessens the privacy of the calling party.

The AUSTEL Discussion Paper describes two ways in which Caller ID can be blocked. These are per-line and per-call blocking and have been described as follows:



- \* *per-line blocking. The phone company masks the Caller ID on the line at the exchange so that it would never appear, except for calls to emergency numbers*
- \* *per-call blocking. If a customer does not want his or her number to appear for a particular call, the Caller ID could be blocked for just that call by punching in a code or pushing a button. Unlike per-line blocking, this leaves the choice in the hands of the caller on a call-by-call basis.*

The Committee concluded that the introduction of a Caller ID service would present significant information privacy problems. The Committee was not convinced that the possible benefits which Caller ID offers are sufficient to justify its introduction.

The Committee considered that if Caller ID is to be offered by telecommunications carriers in Australia, then blocking options must also be made available. The preferred blocking option from the Committee's viewpoint is per-call disclosure whereby the calling party can choose whether to disclose calling line information on a per-call basis.

#### Automatic Calling Equipment

Automatic calling equipment (ACE) is the generic description for a range of equipment which does some or all of the task of setting up phone calls. The AUSTEL Discussion Paper highlights telemarketing machines as an example of ACE. Telemarketing machines use a computerised database of telephone numbers to make calls and can store the numbers which are busy or unanswered for later calling. While the Committee understands that telemarketing machines are not yet common in Australia, it is concerned at the scale of intrusion ACE could permit if it is not properly regulated.

In its submission, the Committee stated that it was concerned about the impact of Automatic Calling Equipment, and that technical standards to limit the intrusion caused by such equipment are necessary.

#### Telephone Information Management Systems

Telephone Information Management Systems (TIMS) have a significant capacity to cause undue harassment and surveillance of employees. TIMS equipment can be used to provide sophisticated monitoring of telephone usage and cost allocation.

In 1983, the Committee, in association with the Labor Council of New South Wales, issued a document *"Guidelines for Telephone Information and Management Systems* (The "TIMS" Guidelines). The Committee considers that there may be a need to update the content and/or form of these guidelines.

#### Telemarketing

Telemarketing is the practice of using unsolicited phone calls or facsimiles for the purpose of promoting or selling products, soliciting donations or conducting market research.

Privacy Committee policy is that such authorities should be limited in duration and only for purposes specified in the authority. The Committee consequently advised that the authority should only authorise liaison with the treating doctor "about my health status in relation to this job application" or words to similar effect.

The Committee also suggested that the final guidelines should provide explicitly that job applicants be informed about the nature and purpose of any medical testing prior to referral to the health assessment provider.

Prior to approval of the draft pre-employment health assessment guidelines by the Premier's Department, the Privacy Committee was asked to provide additional comment.

The Committee suggested a number of changes to the text which were intended to highlight the data protection and privacy issues. Amendments suggested by the Privacy Committee were adopted by the Premier's Department in the final text of the guidelines which was released in September 1992.

The guidelines will become the basis for the pre-employment health assessment within all New South Wales public service organisations.

## 5.2 Pre-Employment Health Assessment Forms

In January 1992, a union approached the Committee for advice on a pre-employment health assessment form being introduced for new employees.

The union was concerned that some of the questions asked may have been in breach of anti-discrimination laws and might also constitute an invasion of privacy.

The Committee recognised that the company's pre-employment health assessment form was not unlike many others already in use in the workplace. However, its main concern was to ensure that the collection of information required by the form was consistent with the Committee's recommended data protection principles.

One such principle is that personal information should only be collected where the information is necessary for or directly related to the purpose of the collection.

The major purpose of the form was to determine whether job applicants are capable of doing the job for which they have applied. The Committee sought to ensure that only health data relevant to the specific duties of employment was being collected rather than a full medical history.

The Committee advised that particular questions on the company's existing form were irrelevant. For example, there were questions about pregnancy termination and cosmetic surgery, responses to which would not be relevant to a general assessment of fitness for employment. Appropriate modification of the form was therefore suggested.



Many of the medical and health files related to research projects. The issues raised included the need to obtain the informed consent of research subjects and the need for care in releasing sensitive information.

The Committee was also called upon to provide advice on proposed laws and amendments to existing legislation including the Data Protection Bill 1992, the Anti-Discrimination Act, the Firearms Act, the Justices Act, the Adoption Information Act and the Liquor and Gaming Acts.

Some examples of the Committee's advisory work are set out in this Chapter.

### 5.1 Pre-Employment Health Assessment Project

In 1992, the Committee gave advice concerning the development of occupational health assessment policies in the New South Wales public sector.

In October 1990 a report was released by an Interdepartmental Working Party set up to review occupational health services provided by the Medical Examination Centre (now called Health Quest). A new public service policy on occupational health assessments, based on the policies as recommended by the Working Party report, was piloted within the Police Service in 1991.

The Privacy Committee supplied detailed comments to Health Quest and to the Premier's Department on the privacy issues raised by the pre-employment health assessment project. It reviewed and commented on draft guidelines for pre-employment health assessments and on the "Baseline Health Questionnaire". The Baseline Health Questionnaire was developed as a means of obtaining basic information necessary to carry out a pre-employment health assessment.

The Committee's primary concern was to ensure that the guidelines made adequate reference to the need for public sector employers and health assessment providers to abide by data protection principles in the conduct of pre-employment health assessments.

The approach adopted by Health Quest seemed broadly consistent with the data protection principles. In particular the Committee noted the following features of the proposed procedures:

- \* the baseline health questionnaire requests only limited information on whether the person considers they can fulfil certain basic health requirements;
- \* health testing requirements are to be limited by reference to the job demands of specific job classifications;
- \* only the preferred applicant for a position is referred for assessment by a health assessment provider.

On completion of the baseline health questionnaire applicants are asked to authorise Health Quest to liaise with their treating doctor about their health status.

Telemarketing is a form of direct marketing. In 1989, the Committee issued a discussion paper on the privacy aspects of direct marketing. The paper concluded that the rapid growth of the direct marketing industry and its use of advanced data processing technology has led to an increased potential for invasions of privacy. The Committee has also encouraged the direct marketing industry to comply with data protection standards.

The Privacy Committee will continue to monitor telemarketing and to consider whether regulation of telemarketing practices is necessary.

### Regulation of Privacy and Telecommunications in Australia

Before the introduction of possibly privacy invasive telecommunications services, the community should be put in the position to make an informed decision on whether the technology should be adopted or not.

The Privacy Committee is concerned that the present regulatory framework may not be adequate to address the privacy challenge presented by new telecommunications technologies and services.

Under the *Telecommunications Act 1991*, AUSTEL's general functions include the protection of consumers from unfair practices of carriers and other persons in the supply of telecommunications services. However, it seems that AUSTEL in performing its regulatory functions has limited ability to take privacy considerations into account. For example, the Committee understands that AUSTEL may not be able to issue permits for the connection of customer equipment to a telecommunications network. This may unduly restrict AUSTEL's ability to regulate services such as Caller ID.

The Committee therefore concluded that privacy should be recognised as a specific issue that must be considered by telecommunications regulators. The Committee also considers it essential that the telecommunications industry be subject to data protection legislation.

The Final Report of the AUSTEL Inquiry was released in December 1992. The major recommendations of the Report were that:

- \* Measures to control the capture and use of personal data by means of telecommunications networks or services should have regard to...general principles or laws governing those matters [this would include privacy laws].
- \* Consideration should be given to extending the scope of the *Privacy Act 1988* beyond its current focus on government bodies to oversee the collection, storage and use of data by private companies.
- \* Subject to additional funding being made available, a Telecommunications Privacy Committee should be set up with responsibility for the identification of general privacy principles applicable to the telecommunications industry; the development of specific guidelines where necessary; encouraging relevant industry and community groups to develop codes of conduct which reflect the general privacy principles and specific guidelines; the approval of codes of conduct which meet appropriate standards, including effective monitoring and enforcement issues.



- \* The principle of "informed choice" should govern the introduction of Calling Line Identification (Caller ID) based services, particularly Calling Number Display.
- \* Appropriate codes of conduct should be developed by relevant industry and community groups for approval by the Telecommunications Privacy Committee to deal with intrusion, control of personal data and fair trading issues in relation to unsolicited telecommunications.
- \* Individuals affected should be informed by appropriate means whenever data resulting from the use of a Telephone Information Management System (TIMS) is being collected and processed.
- \* Compilers and purchasers of reverse directories should develop a code of conduct that recognises the sensitivity of a reverse telephone directory compared to one that can only be accessed, when the name of the subscriber is known.

The Privacy Committee will continue to monitor developments which arise from the implementation of the Final Report.

## Chapter 5

### ADVICE

#### 5.0 Introduction

The Privacy Committee Act 1975 empowers the Committee to: "make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons" (section 15(1)(c)).

The majority of the Committee's reports and recommendations arise out of requests for advice. Each year, the Committee receives a large number of requests for advice from local, State and Commonwealth government agencies, community groups, unions, business and professional associations, legal and medical practitioners, universities, technical colleges and other educational institutions as well as from various agencies in other countries and from members of the public.

The Committee does not always wait until a request is received before it offers its advice. From time to time, a media announcement or complaint will alert the Committee to a matter that requires immediate attention. In such cases, the Committee will approach the organisation or individual concerned and seek further information about the matter so that appropriate recommendations can be made.

The Committee also provides information to students, researchers and writers with an interest in privacy related issues. A specialised library and stock of Committee publications is maintained to assist in providing this service. Because of the Committee's reputation and lengthy experience in the field, requests for information are received from all States of Australia, from overseas as well as from individuals and organisations in New South Wales.

During 1992, the Committee opened 282 Advice files and carried forward 86 files from previous years. A total of 309 files were completed in 1992 and 59 matters were to be carried forward into 1993.

Of the requests for advice received by the Committee in 1992, 63% came from government agencies and 37% came from the private sector and the general public.

The significant categories of requests for advice were as follows:-

* Employment	12%
* Medical and Health	11%
* Laws and Legislation	9%
* Transport and RTA records	7%
* Police Courts and Law Enforcement	6%
* Direct Marketing	6%

Employment privacy issues featured as an area of general concern. Requests for advice to the Committee reflect an increasing sensitivity on the part of some employers, personnel consultants and unions towards the potential for privacy invasion in this field and the need to anticipate and resolve any problems which might arise.



P. Hamilton

PRIVACY COMMITTEE  
OF NEW SOUTH WALES

For list of  
publications

Adding 1992 report  
to me  
6-6-84

1991 ANNUAL REPORT



The Hon. J. Hannaford, M.L.C.,  
Attorney General and Minister for  
Industrial Relations,  
Level 20,  
Goodsell Building,  
8 - 12 Chifley Square,  
SYDNEY, N.S.W., 2000

Dear Mr. Hannaford,

In compliance with Section 17 of the Privacy Committee Act 1975, the Privacy Committee has the honour to submit its Annual Report for the year 1991.

T. Cohen (Chairman)  
J. Morgan (Executive Member)  
D. Dale  
H. Gamble  
W. Haylen, Q.C.  
L. Lawrence  
I. Macdonald, M.L.C.  
M. Norsa  
D. Temple  
A. Tink, M.L.A.  
B.R. Vermeesch

---



## CHAIRMAN'S PREFACE

It is not usual for Privacy Committee annual reports to include a Chairman's preface. However, two matters of considerable importance have arisen which merit comment before the Committee next reports to Parliament.

The first concerns the release of the report by the Independent Commission Against Corruption (ICAC) on the Unauthorised Release of Government Information in August 1992. The report provides details of the massive, multi-million dollar illicit trade in government information involving police, public servants, insurance companies, banks, financial institutions, lawyers and private investigators.

The report reveals that the type of information traded included addresses, silent telephone numbers, bank account and pension details, social security information, medicare records, criminal history information and details of people's movements in and out of the country.

The sources of information included the Roads and Traffic Authority, the Departments of Social Security, Immigration and Customs, Australia Post, Telecom and the New South Wales Police Service.

A total of 155 people were found to have engaged in corrupt conduct and a further 101 to have engaged in conduct which allowed, encouraged or caused the occurrence of corruption.

The report clearly shows that the right to privacy, specifically information privacy, has neither been respected nor protected in government and business circles and the privacy of tens of thousands of people has been breached.

On the subject of the right to privacy, the ICAC report has this to say:

*"substantial weight must be given to the right to privacy in the formulation of laws and procedures governing the handling of information. It cannot be dismissed as a mere catchcry of civil libertarians. It is an internationally recognised right."*

The 14 recommendations made in the ICAC report are directed - quite properly - to the elimination of corrupt conduct and they do not pretend to be a complete answer to the privacy issues identified in the report.

The Privacy Committee has prepared a report which outlines what is needed to ensure that the privacy rights of the citizens of New South Wales are adequately protected. This report, entitled 'Privacy and Data Protection in New South Wales - A Proposal for Legislation (summarised in Chapter 4) calls for the immediate introduction of data protection legislation backed up by a properly resourced and independent supervisory authority.

The Attorney General, Mr. Hannaford, has responded to the revelations of the ICAC inquiry by announcing that he intends to introduce data protection legislation as soon as possible. Since this announcement, the Attorney General's Department has been consulting with the Committee about the content of the legislation.

43. The Department of Motor Transport - Personal Data Systems in the New South Wales Public Sector (April 1978)
44. Blacklists: Finding a Fair Balance of Interests (January 1978)
45. The New South Wales Police Special Branch (March 1978)
46. \*International Legislation for Privacy Protection in Data Systems (Implications for Australia)(June 1978)
- 47b. Lie Detectors (April 1979)
- 48a. The Collection, Storage and Dissemination of Criminal Records by the Police (November 1978)
- 49a. Guidelines for Debt Collection (August 1979)
- 49b. Police Department On-Line Availability of the Criminal Names Index (August 1979)
50. Consumer Credit Reporting: An Overview (November 1979)
51. Commercial Credit Reporting: An Overview (February 1980)
52. \*Police Department On-Line Access to Department of Motor Transport Traffic Convictions Records (April 1979)
53. Telephone Usage Monitoring Systems (TIMS)(November 1983)
54. Acquired Immune Deficiency Syndrome (AIDS) - Guidelines for the Testing of Antibodies to HTLV-III (AIDS) Virus (February 1986)
55. Privacy Issues and the Proposed National Identification Scheme (March 1986)
56. Submission to the Joint Parliamentary Select Committee on Telecommunications Interception (September 1986)
57. The Medical Examination Centre (March 1987)
58. National Identification System - A Further Report (February 1988)
59. Direct Marketing - Discussion Paper (April 1989)
- 60A. Report on Regulation of Credit Reporting (March 1989)
- 60B. Further Report on Regulation of Credit Reporting (September 1989)
61. Privacy Law in the Information Age - Seminar Proceedings (June 1990)
62. Electronic Vehicle Tracking Issues Paper (August 1990)
63. Privacy and Data Protection in New South Wales - A Proposal for Legislation (June 1991)



27. \*Report on the Public Service Board Criminal Checks in Employment (November 1976)
28. Personal Data Systems in the New South Wales Public Sector Totalizator Agency Board (November 1976)
29. Unsolicited Telephone Calls (September 1978)
30. Survey of Personal Data Systems in the New South Wales Public Sector (January 1977)
31. Guidelines for the Operation of Personal Data Systems (March 1986)
32. Submission to the Australian Law Reform Commission Regarding the Census (April 1977)
33. Submission to the Criminal Investigation Bill 1977 (Commonwealth)(May 1977)
34. Does the Privacy Committee consider that a register of pecuniary interests should be introduced? Submission to the Joint Committee of the Legislative Council and Legislative Assembly upon pecuniary interests (June 1977)
35. Research and Confidential Data: Guidelines for Access (May 1986)
36. The Medical Examination Centre (October 1977)
37. Defamation and Privacy: Submission of the New South Wales Privacy Committee on the Proposals of the Australian Law Reform Commission (Against 1977)
38. Personal Data Systems in the New South Wales Public Sector - State Electoral Office (August 1977)
- 39a. Employment Guidelines - The Privacy Aspects of Employment Practices in the Private Sector (October 1979)
- 39b. Employment Background Paper: The Privacy Aspects of Employment Practices in the Private Sector (October 1979)
- 39c. Openness in the Employee-Employer Relationship to Ensure Fairness (March 1979)
40. Consumer Affairs Motor Dealers Inspectors Access to DMT Motor Vehicle Registration Records (November 1977)
- 41a. \*The Use of Criminal Records in the Public Sector (November 1977)
42. Guidelines for Surveys (January 1978) *See Nov 1979*

This undertaking to give information privacy statutory protection is welcomed by the Committee as it has been advocating the enactment of such legislation for more than 10 years.

The second matter which requires comment is the vexed issue of the Committee's lack of resources. The Committee has reluctantly concluded that it is simply not possible to conduct research into important privacy issues and to meet all the requests for advice it receives with the services of just three research officers and one administrative assistant. The Committee has carefully evaluated which advice and research projects need to be given priority because of the importance of the issues they raise and the numbers of people they affect. It has also taken a hard look at what can realistically be achieved within existing resources. An unfortunate result of this assessment of priorities is that clients of the Committee, who have sought or are seeking advice on matters which are not priorities, are being advised that, owing to competing demands and insufficient resources, the Committee is unable to assist them at this time. Where possible, clients are given copies of any relevant Committee guidelines to help them with the matters they have raised. But guidelines do not exist on every privacy issue and many of the Committee's existing guidelines were drafted in the seventies and now need urgent revision.

Clearly, the situation is most unsatisfactory.

In New South Wales, in stark contrast to the hundreds of millions of dollars which are invested each year in information technology, there is virtually no financial commitment to the protection of privacy. The people of this state have paid dearly for 'privacy on the cheap', as evidenced by the revelations of the ICAC report.

It is hoped that the passage of data protection legislation will result in an appropriate increase in the resources allocated to privacy and data protection.



Mrs. Totti Cohen  
CHAIRMAN



### The Privacy Committee's Goal

The promotion and protection of the privacy of persons in New South Wales:

The Privacy Committee, a statutory body constituted under the Privacy Committee Act 1975, No. 37, works to achieve its goal by:

- Promoting and protecting the privacy of persons in New South Wales through the conduct of research, the provision of advice, and the preparation of reports and recommendations on privacy policy issues to the government and the community.
- Promoting the adoption and implementation of privacy protection programs.
- Answering inquiries and investigating allegations of breaches of privacy of persons and undertaking conciliation and resolution of complaints.
- Preparing and disseminating information on privacy issues and providing educational material and media comment on topical privacy issues.
- Managing allocated funds, staff and other resources to ensure efficient and effective achievement of legislative goals.

5. Universal Identification Numbers (July 1975)
6. National Compensation Bill 1975 (August 1975)
7. Medibank Privacy Issues (Submission Relating to the Health Insurance No. 2 Bill, 1975)(August 1975)
8. \*Defamation and the Granting of Credit (August 1975)
9. Press Councils (September 1975)
10. Rehabilitation of Offenders (June 1976)
11. \*Enforcement of Money Judgements (includes submission to the New South Wales Law Reform Commission)(October 1975)
12. Submission to the Royal Commission on Intelligence and Data Security (January 1976)
13. Problems in Consumer Credit Report (February 1976)
14. A Report on Consumer Access to Credit Bureau Records in New South Wales (April 1976)
15. Personal Data Systems (February 1976)
16. Overseas proposals Relating to the Regulation of Personal Data Systems (April 1976)
17. Programme for Study of Medical Privacy (February 1976)
18. \*Programme for Study of Privacy Aspects of Employment Practices (February 1976)
19. \*Criminal Records and their Uses in New South Wales (September 1976)
20. Research Materials held by the Committee (September 1976)
21. \*Bibliography: Extra-Judicial Debt Collection (May 1976)
22. A Summary of the Morison Report on the Law of Privacy (Tabled April, 1973)(April 1976)
23. Legislation Concerning Educational Records in the USA (August 1984)
24. Individual Identification (September 1976)
25. Mandatory Reporting of Child Abuse (September 1976)
26. Unsolicited Mail and Leaflets (September 1976)



## APPENDIX 3

## List of Publications

A. ANNUAL REPORTS

1975 - 1990

B. THE PRIVACY BULLETIN

Volume 1 No. 1 March 1985  
 Volume 1 No. 2 July 1985  
 Volume 1 No. 3 December 1985

Volume 2 No. 1 July 1986  
 Volume 2 No. 2 September 1986

Volume 3 No. 1 February 1987  
 Volume 3 No. 2 May 1987  
 Volume 3 No. 3 November 1987

Volume 4 No. 1 July 1988  
 Volume 4 No. 2 November 1988  
 Volume 4 No. 3 December 1988

Volume 5 No. 1 November 1989

Volume 6 No. 1 April 1990  
 Volume 6 No. 2 August 1990  
 Volume 6 No. 3 September 1990

Volume 7 No. 1 April 1991  
 Volume 7 No. 2 May 1991

C. REPORTS

1. Integrated Data Systems (Commonwealth - Crisp Report)(May 1975)
2. \*The Credit Industry - Granting of Credit and Credit Bureaux (May 1975)
3. \*Australian Criminal Information Centre (May)
4. \*Criminal Information Systems - Submission to the Australian Law Reform Commission (July 1975)

## THE PRIVACY COMMITTEE

The Committee is responsible for the whole range of privacy issues in both the public and the private sectors.

Established by the Privacy Committee Act 1975 (NSW), it commenced operations on 2nd May, 1975.

It is a statutory Committee independent of government, which acts as a privacy ombudsman.

Section 5 (2) of the Privacy Committee Act states that: 'The Committee shall consist of not less than twelve nor more than fifteen members' who are selected in accordance with a formula set out in the Act.

## COMMITTEE MEMBERS

<b>Totti Cohen</b>	AM, OBE, Solicitor, Chairman
<b>Jacqueline Morgan</b>	Executive Member
<b>David Dale</b>	Journalist
<b>Helen Gaible</b>	Professor of Legal Studies, University of Wollongong
<b>Andrew George</b>	Deputy Director General, Attorney General's Department
<b>Wayne Haylen</b>	Queen's Counsel
<b>Les Lawrence</b>	Computer Consultant
<b>Ian Macdonald</b>	Member of the Opposition
<b>Michael Norsa</b>	Computer Consultant
<b>Diana Temple</b>	Associate of the Department of Pharmacology, Sydney University
<b>Andrew Tink</b>	Government Member
<b>Bob Vermeesch</b>	Deputy Chairman, Commercial Tribunal

## STAFF OF THE COMMITTEE

<b>Jacqueline Morgan</b>	Executive Member
<b>Maureen Tangney</b>	Director, Research and Policy
<b>Diane Johnson</b>	Investigations Officer
<b>Bruce Alston</b>	Research Officer
<b>Karyn Edelstein</b>	Research Officer
<b>Liz Atkins</b>	Executive Assistant
<b>Stella Percival</b>	Commonwealth Trainee
<b>James Hmelnitzsky</b>	Research Officer (April to September 1991)
<b>Penny Quarry</b>	Research Officer (from March 1991)
<b>Justine Roberts</b>	Secretarial Assistant (April to September 1991)
<b>Eleanor Lees</b>	Commonwealth Trainee (from December 1991)



## FUNCTIONS OF THE COMMITTEE

Section 15 (1) of the Privacy Committee Act sets out the powers, duties and functions of the Committee as follows:

"15 (1) Subject to this Act, the Committee -

- (a) may conduct research and collect and collate information in respect of any matter relating to the privacy of persons;
  - (b) may and, if directed by the Minister so to do, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of persons;
  - (c) may make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons;
  - (d) may receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;
  - (e) may, in relation to any matter relating to the privacy of persons generally, disseminate information and undertake educational work;
  - (f) may, in relation to any matter relating to the privacy of persons generally, make public statements; and
  - (g) may, for the purposes of this Act, conduct such inquiries and make such investigations as it thinks fit.
- (2) The Committee shall, from time to time when requested by the Minister, prepare and submit to the Minister programmes for the examination of matters relating to the privacy of persons and pursue those programmes in such order, if any, as is determined by the Minister and notified by him to the Committee.
  - (3) Any member of the Committee may submit to the Minister a minority report or recommendation on any matter in respect of which the Committee makes a report or recommendation to the Minister."

## APPENDIX 2

## Attendance at Full Committee Meetings

		Attendance	Number Entitled to attend
<b>Chairman:</b>	T. Cohen	9	10
<b>Executive Member:</b>	J. Morgan	9	10
<b><u>Members:</u></b>			
	D. Dale	4	10
	H. Gamble	6	10
	A.J.B. George	7	10
	W. Haylen	1	10
	L. Lawrence	7	10
	I.M. Macdonald	5	10
	M. Norsa	7	10
	D. Temple	9	10
	A. G. Tink	5	10
	B.R. Vermeesch	5	10



## APPENDIX 1

## Budget Expenditure and Allocation

	Actual Expenditure 90/91	Allocation 91/92
	\$000	\$000
Salaries Etc.	262	270
National Wage Provision	0	0
Leave on Retirement	6	1
Overtime	0	0
Workers Compensation	3	3
Personal Accident Insurance	0	0
Meal Allowances	0	0
Payroll Tax	17	18
Fringe Benefits Tax	0	0
Employers Super Contribution	36	0
Payments in Nature of Salaries	324	292
Rent	117	118
Rates, Charges Etc	0	0
Maintenance of Buildings	0	0
Insurance	0	0
Cleaning	0	0
Travelling Expenses	1	2
Motor Vehicle Expenses	0	0
Freight, Cartage Etc	0	1
Advertising and Publicity	0	0
Books Paper Etc	6	6
Fees for Services Rendered	17	22
Gas and Electricity	3	4
Laundry Expenses	0	0
Other Insurance	0	0
Postal and Telephone Expenses	4	4
Printing Expenses	12	18
Stores, Provisions, Etc	21	3
Minor Expenses	0	1
Out of Pocket Expenses	0	0
Maintenance Contracts	0	3
Maintenance and Operating Expenses	181	182
Total	505	474

## TABLE OF CONTENTS

## CHAPTERS:

1.	<u>Introduction</u>	9
2.	<u>Administration</u>	11
2.0	Introduction	11
2.1	Membership and Meetings of the Committee	11
2.2	Staff of the Committee	11
2.3	Committee Resources	12
2.4	Departmental Administration	12
2.5	Priorities	13
2.6	Delegations	13
2.7	Membership of Other Committees and Statutory Bodies	14
3.	<u>Promoting Privacy</u>	15
3.0	Introduction	15
3.1	Media	15
3.2	Speaking Engagements	15
3.3	Publications	16
3.4	Privacy Agencies	17
3.5	Visitors	18
3.6	International Contacts	18
4.	<u>Significant Issues of 1991</u>	19
4.0	Introduction	19
4.1	Independent Commission Against Corruption - Operation Tamba	19
4.2	Data Protection Bill	23
4.3	Privacy and Personnel Records	24
4.4	Criminal Records Act	27
4.5	Credit Reporting	29
4.6	Privacy Law Reform in Other States	30
5.	<u>Advice</u>	32
5.0	Introduction	32
5.1	"Outing" Policy Statement	23
5.2	Video Surveillance of Public Places by Police	
5.3	Criminal Record Checks	34
5.4	Police Reports on Applicants for Drivers' Licenses	36
5.5	Underage Drinking Infringement Notices	37
5.6	Disclosure of Student Results to Residential Colleges of the University of Sydney	38
5.7	Casino Inquiry	38



5.8	Disclosure of Registry of Births, Deaths and Marriages Information to the Australian Institute of Health	39
5.9	National Health and Medical Research Council - Guidelines for the Protection of Privacy in the Conduct of Medical Research	40
5.10	Public Access to State Electoral Rolls	41
5.11	Commonwealth Data Matching Using State Records	42
5.12	State Land Information Council	43
5.13	Law Enforcement Access Network	44
5.14	Privacy of Equal Employment Opportunity Data	45
5.15	Telecommunications and Privacy	47
5.16	Occupational Health Assessments	47
<b>6.</b>	<b><u>Complaints</u></b>	<b>49</b>
6.0	Introduction	49
6.1	Resolution of Informal Complaints	49
6.2	Resolution of Formal Written Complaints	50
6.3	Statistics	50
6.4	Some cases:	52
	• Video Shop Membership	52
	• Stolen Vehicle Claim	52
	• Mistaken Credit Report	53
	• Confidential Information Disclosed	53
	• Access to Credit Record	54
	• Locating Debtor, Court Case and Other	55
	• Refusal to Release Original Medical Records	55
	• Disclosure of Representations on Behalf of Constituents	55
	• Disclosure of Bank Account Details	56
	• Disclosure of New Address	56
	• Window-Faced Envelopes	57
	• Frequent Telephone Calls	57
	• Letters of Demand	58
	• Adoption	58
	• Assessing Application for Employment	59
	• Registrar of Race Horses	59
	• Unsolicited Mail from Overseas	60
	• Connected to Former Husband	60
	• Employment References	61

#### APPENDICES:

1.	Budget Expenditure and Allocation	62
2.	Attendance at Full Committee Meetings	63
3.	List of Publications	64

information. She was also concerned that her own account may in some way be still connected to her former husband.

The bank advised that the mailing list had been supplied by a mailing house list broker. The name and address of the complainant's former husband was used as part of a test run for quality control. This means that his name was pulled at random from over 30 lists that the bank rented for that mailing. To identify exactly which list his name came from would require reconstruction of these lists. Part of the bank's agreement with the list brokers was that the lists would not be kept after a mailing.

To overcome this problem, the bank has introduced a new procedure for future mailings. A code will be included on the letters of solicitation which will enable the relevant mailing list to be identified, even if the list is used in a random test. The Committee considered the new procedures to be acceptable.

#### Employment References

A complaint was received about a negative reference being passed on to prospective employers by a former employer. The complainant was in a bind. He had worked for the former employer for a number of years but resigned after a personality clash with a new manager. It was not feasible to omit the former employer as a referee, but the negative character reference was not improving his employment prospects.

The Committee contacted the former employer on the complainant's behalf. The employer agreed that there was no actual evidence on which to base the negative information being provided to enquirers. It was agreed, after negotiation, that a reference to a prospective employer making enquiries regarding the complainant would simply confirm his period of employment. The complainant was satisfied with this arrangement.



In response to the Committee's request for comment, the Registrar replied that the date of birth was required for identification purposes. It was not uncommon for members of one family, often with the same name, to own race horses, or for separate individuals to have the same or similar name. The date of birth was seen as an effective method of distinguishing individuals. The Committee considered the explanation to be reasonable. The Committee has no objection to the collection of date of birth information when it is necessary for identification purposes.

### Unsolicited Mail from Overseas

The Committee continues to receive complaints regarding the receipt of unsolicited mail from overseas. Much of the promotional material relates to overseas lottery ticket sales. The complainants are usually concerned about how an overseas company was able to find out their name and address.

The Committee has ascertained that overseas companies generally obtain the information from computerised public record information or mailing house list brokers.

In fact Australia Post, in its publication "List of Lists", provides details of over 2000 lists available through mailing house list brokers and compiled from various sources. It is the practice of many private sector organisations to sell names and address information to list brokers for a fee.

The Committee is concerned about the non-consensual disclosure of information by organisations for direct marketing purposes. Committee policy is that, in general, information collected for one purpose should not be used for another purpose without the consent of the information subject.

The Committee considers, according to its current guidelines, that an individual should be able to have personal particulars removed from an organisation's mailing list. The Committee also considers that the individual should be able to know the source from which the personal particulars were obtained.

Unfortunately, in the case of material received from overseas the Committee does not have the statutory powers to undertake enquiries into complaints received about foreign organisations. However if the original source of the mailing list used by the foreign organisation can be identified as a New South Wales organisation the Committee will investigate.

### Connected to Former Husband

The complainant had been divorced for over ten years and was not on good terms with her former husband. When she received a promotional letter addressed to her former husband from her bank she was most annoyed. She wanted to know how the bank could have obtained such out of date

## Chapter 1

### INTRODUCTION

Last year the Committee reported that personal information provided in good faith (and frequently under legal compulsion) to government agencies was being bartered and sold by public servants, police, private investigators, insurance companies, banks and other financial institutions. This trade was being investigated by the Independent Commission Against Corruption and the investigation continued throughout 1991.

ICAC sought the Committee's advice on the data protection issues raised by its investigation. Of course, the Committee was more than happy to oblige and in June 1991 submitted a report which not only addressed the specific issues raised by ICAC, but also included a model for effective privacy and data protection legislation. A copy of this report was sent to every Parliamentarian.

Our elected representatives now face a very important challenge. Privacy, after all, is one of the most fundamental values of a liberal democracy. Once it is lost, it cannot easily be retrieved. If Parliament fails to act decisively to protect privacy, then the outlook for the future is not bright.

There will be nothing to stop the relentless accumulation of personal information in databases. Nothing to stop this information from being swapped, bought and sold for any number of purposes, without the knowledge or consent of the people to whom the information relates. Nothing to protect people from the harm that can be caused when inaccurate information finds its way into records, whether by human or computer error or by malice. Nothing to stop new means of computer assisted surveillance penetrating ever deeper into our society.

At the end of 1991 a Data Protection Bill was introduced into Parliament. It is a private member's Bill - not a Government bill - and debate on the Bill is not expected to commence until ICAC releases its report on the unauthorised release of government information in 1992.

The Bill incorporates the data protection principles which were set out in the Committee's model for privacy and data protection legislation. Unfortunately, very little else of the Committee's proposal is reflected in the Bill.

If enacted in its present form the Bill would give each departmental head the power to exempt individual records or classes of records of personal information from any or all of the data protection principles. This will only lead to inconsistency and confusion among government departments.

We do not need half measures - we need legislation which shows a strong commitment to privacy. We need legislation which allows us to control the tremendous power that has been unleashed by developments in information technology, so that the technology helps and does not harm us.

When parliamentary debate on the Data Protection Bill begins, there is likely to be a great deal of talk about the need to balance interests which compete with privacy, such as the need for government and business to operate efficiently.



Of course there is a need for balance. At the moment, however, a huge correction in favour of privacy is needed to achieve anything approaching balance. This is evident from ICAC's hearings which provided ample proof that privacy is neither respected or protected within many government and business institutions.

The Privacy Committee was set up for the very purpose of making reports and recommendations about what legislative and administrative action needs to be taken to protect privacy. The Committee has done its part and has given Parliament a model for the necessary legislation.

Now is the time for action.

2. medical history information should only be released where necessary for the effective care or treatment of an adopted person.

In 1991, the state government announced that the operation of the Act would be subject to review by the New South Wales Law Reform Commission.

### Assessing Application for Employment

The complainant was upset as he had been declined employment with the Department of Corrective Services on the basis of a minor criminal offence which was more than ten years old. He was aware of the Criminal Records Act 1991 which had been passed by the New South Wales government in April 1991, and could not understand why his prior record had been taken into account when assessing his application for employment.

The purpose of the Criminal Records Act to limit the effect of a person's conviction for a relatively minor offence if the person completes a period of crime-free behaviour, i.e., 10 years. On completion of the period, the conviction is to be regarded as spent and, subject to some exceptions, is not to form part of the person's criminal history.

Section 12 of the Act outlines the provisions where a conviction is considered spent. In general the consequences of a conviction becoming spent, means the person is not required to disclose to any other person for any purpose information concerning the spent conviction. In addition a question concerning the person's criminal history is taken to refer only to convictions of the person which are not spent.

The legislation does however have a number of exclusions. For example, Section 15(1) states:

*"Section 12 does not apply in relation to an application by a person for appointment or employment as a judge, magistrate, justice of the peace, police officer, prison officer, teacher, teachers aide or a provider of child care services under Part 3 of the Children (Care and Protection) Act 1987."*

In this case, the complainant was seeking employment as a prison officer, and so the Committee was obliged to point out that the Department of Corrective Services could take the old convictions into account.

### Registrar of Race Horses

The Committee receives numerous complaints about requests by organisations for date of birth information. In this case the complainant was a race horse owner and his date of birth had been requested by the Registrar of Race Horses. The complainant could not see how his age was relevant to his ownership of a race horse.



## Letters of Demand

The complainant was having problems with a finance company which continued to send letters of demand to him regarding an unpaid account owed by his grandson. The complainant's grandson had lived at his grandparent's home for a year. He had since fallen out with them and moved interstate.

The complainant had told the finance company this and had given it the last known address he had for his grandson. The complainant was in no way a party to the contract nor was he legally liable for the debt. The finance company continued to send letters of demand to the complainant's address and then later to telephone, demanding to know the grandson's whereabouts. The complainant asked the Committee for help.

The Committee contacted the finance company who stated that the account had been placed in the hands of a loss recovery agency and they were not aware of the agency's actions. The finance company agreed to tell the agency to cease contacting the complainant.

## Adoption

During 1991 the Committee received many enquiries regarding the Adoption Information Act which came into effect in April 1991.

The Act allows greater access to information about adoptions. For example, it gives adopted children and their birth parents the right to obtain identifying information about each other once the child turns 18.

Most of the people who made enquiries or complaints about the new law to the Committee, were adoptive parents who were concerned that the law would adversely affect their adopted children.

All enquirers were advised that the right to access identifying information did not come into effect until an adopted child had reached adulthood. At that time, the then adult adoptee and his or her birth parents could choose to lodge a contact veto if they did not wish contact to be made with the other party.

Enquirers were also advised that whilst the Committee supports the right of adoptees and their birth parents to know each others' identity, the Committee does not believe that other social history information should be made available without the record subject's informed consent.

The Committee has recommended that:

1. in the absence of the data-subject's consent, only information which is necessary to establish the identity of a party to an adoption should be released;

## Chapter 2

### ADMINISTRATION

#### 2.0 Introduction

Privacy Committee members are appointed by the Governor on the advice of the government of New South Wales. The Committee consists of no less than 12 and no more than 15 members. The Act provides for one member to be the Executive Member of the Committee. Of the appointed members, one must be from the Government and one from the Opposition, two must be employees of universities and no more than two are to come from the New South Wales public service.

The Committee's powers cover both the public and private sectors. They are set out in section 16 of the Privacy Committee Act 1975, and include the power to require any person to attend and give evidence or produce documents. In conducting any inquiry or investigation, the Committee has the powers, protections and immunities conferred on a Commissioner by Division 1 of Part II of the Royal Commissions Act 1923. The Privacy Committee has no power to enforce its recommendations, but may make reports to Parliament under sections 17 and 18 of the Privacy Committee Act 1975.

#### 2.1 Membership and Meetings of the Committee

Membership of the Committee continued unchanged during the year.

In 1991, the Full Committee met on 10 occasions.

#### 2.2 Staff of the Committee

The Committee's full-time staff number, at six, remained unchanged during 1991.

Staff members are required to investigate complaints, undertake research and provide advice on privacy issues and also to undertake clerical and administrative tasks.

Throughout 1991, Dr. Jacqueline Morgan and Ms. Maureen Tangney continued in their respective positions of Executive Member and Director of Research and Policy. Ms. Diane Johnson continued as the Investigations Officer. The Committee's Research Officers were Mr. Bruce Alston and Ms. Karyn Edelstein. Secretarial assistance was provided by Ms. Liz Atkins, the Executive Assistant.

Ms. Penny Quarry was seconded from the Attorney General's Department in March 1991 to assist the Committee with its research in reviewing the recordkeeping practices of the Special Branch of the Police Service. Mr. James Hmelnitzsky was a general research assistant from April to September and of special assistance with translation of German documents.



Temporary secretarial assistance was provided intermittently during the year. Ms. Justine Roberts provided assistance particularly for the Special Branch project.

The Committee again participated in the Commonwealth trainee programme with Ms. Stella Percival working for the Committee as a clerical trainee throughout the year and Ms. Eleanor Lees following her as a trainee in December 1991.

### 2.3 Committee Resources

Last year, the Committee reported that it was allocated a budget of \$511,000 for the year 1990-91. This year, the allocation has been reduced to \$474,000 (See Appendix 1).

Despite appearances, this does not amount to a \$37,000 cut to the Committee's operating expenses. Rather, it reflects new arrangements for the payment of superannuation contributions, a mandatory 1.5% productivity saving on salaries, and altered charges for the rent of premises.

In practical terms, the effect of the budget cut is that for the year 1991-92 the Committee will have \$2000 less to spend on operating expenses such as postage and freight.

The Committee's budget is so lean there is really no scope to meet expenses associated with the repair, replacement and upgrading of equipment, the employment of temporary staff and the reprinting of reports when existing stocks run out. With such limited resources, the Committee always finds it difficult to meet the demands made upon it by the community, and never more so than when it receives a request for advice which would involve the Committee in considerable research and the production of a report.

So it was with a great sense of relief that the Committee accepted a special grant of \$25,000 from the Independent Commission Against Corruption (ICAC). The ICAC made these funds available to the Committee to enable it to prepare a detailed submission on the privacy and data protection issues raised by the Commission's inquiry into the unauthorised release of confidential information by government agencies. With these funds, the Committee was able to employ the additional research and clerical staff needed to prepare the report, with minimum disruption to the Committee's other projects.

### 2.4 Departmental Administration

The Executive Member attended 10 meetings and a special conference with officers of the Attorney General's Department concerning corporate planning for the Department.

experience, however, that confidential information is often released by organisations because insufficient care is taken in establishing proper verification procedures because subterfuge is used by the requester, or an employee is acting dishonestly.

The Committee was unable to establish where the federal agency obtained the complainant's address.

### Window-Faced Envelopes

The complainant objected to the way in which he had received a court order. The notice was sealed into a window-faced envelope in such a way as to display that he was a defendant, and the offence with which he was charged. The complainant felt this was an unacceptable embarrassment.

The Committee approached the court concerned on the complainant's behalf. The Committee was informed that most forms in general use are designed for posting in window-faced envelopes to ensure that only the name and address are disclosed. In this case the particular order form was not specifically designed for posting, and staff were instructed not to post the orders in window-faced envelopes. However, as the forms were processed in a high volume area, mistakes did occur. On the advice of the Committee, the registrar of the court agreed to have the forms redesigned so that the sensitive information would not be disclosed by a window-faced envelope.

### Frequent Telephone Calls

The complainant was distressed because a finance company was making frequent telephone calls about an outstanding joint account to his wife's place of work. He had contacted the finance company and was trying to catch up on outstanding payments but the calls continued. He felt that the telephone calls were a deliberate harassment to try to force him to make additional payments.

Generally, the Committee does not have any objection to a finance company contacting a customer at their place of work, as the Committee acknowledges that in many cases this may be the only contact point during office hours. The Committee does object, however, to disclosure by the finance company of account particulars to third parties without the customer's consent. The complainant conceded that the finance company had not disclosed any details of the account or the arrears, but the frequency of the telephone calls was embarrassing. Acting on the Committee's advice, the complainant contacted the finance company which agreed to stop the calls as long as regular payments were made.



The state government minister advised that it was his policy to pass the representations to the local state member as the issues addressed generally came within the local member's domain. The minister was not, initially, inclined to depart from this policy.

The Committee was able to suggest an alternative policy that proved acceptable to both parties. The policy was amended so that, in order to protect privacy, constituents would be given the opportunity to consent before their representations are forwarded to the local member.

### **Disclosure of Bank Account Details**

A number of complaints were received from consumers regarding the alleged disclosure by a bank of customers' account numbers to a credit card company.

The Committee reviewed the arrangement and decided that, since the promotional material was sent by the bank to its account holders, there was no breach of account holders' confidentiality. The Committee was advised by the bank that no information regarding account holders was provided directly to the credit card company.

The Committee raised no objection to the inclusion of the account number in the correspondence, as it was necessary for the identification of the account being referred to, and to ensure that the information was being supplied to the correct account holder.

### **Disclosure of New Address**

The complainant was very alarmed. A federal government investigative agency had contacted her, seeking to find out her former husband's whereabouts. She was now divorced and had gone to some lengths to ensure that her new address was not known to anyone. The complainant was concerned about how the agency had found her new address. She was also worried that if the agency could find her, so could her former husband, or some of his less than desirable acquaintances. The only people she had given the address information to were the staff of the Rental Bond Board.

The Committee contacted the Rental Bond Board to find out whether the address information was released to a third party. The Board advised that no information is given out except to the parties concerned, i.e., agent or landlord or tenant. In all other circumstances legal authority to obtain the information is required. A record of all information released under legal authority is maintained by the Board.

The Board had no record of this particular agency requesting information about the complainant. The Committee was unable to establish where the agency obtained the particulars. In this case, the Committee was satisfied that the Board had suitable data protection procedures in place. It is the Committee's

Committee staff also met with officers of the Attorney General's Department to discuss various management issues including Equal Employment Opportunity policy practice and procedure.

The Committee continues to provide a monthly report as part of the Department's corporate planning and performance assessment programmes.

## **2.5 Priorities**

The Privacy Committee has adopted the following criteria to guide its evaluation of work priorities:

- ★ The Committee should not unnecessarily commit resources to projects already being undertaken by other organisations and interest groups;
- ★ The project should be effective in terms of:
  - resources (including ability of staff, timeliness of advice report, relationship with other current or completed projects);
  - degree of impact on privacy intrusive activities;
  - increased community awareness and capacity of individuals to protect their own privacy interests.
- ★ The project should relate to a matter affecting privacy which is of concern to the community.
- ★ The project should address developments in technology which raise important privacy issues.
- ★ The project should relate to a government initiative or have been referred by a Minister for a Department.

During the year two major projects received priority. These were the preparation of a submission on privacy and data protection to the Independent Commission Against Corruption and the review of recordkeeping practices of the Special Branch of the Police Service.

## **2.6 Delegations**

Section 14 of the Privacy Committee Act 1975 permits the delegation of any of the powers, authorities, duties or functions of the Committee. Delegation of the Committee's powers to compel testimony and or the production of books or documents is only permitted with the approval of the Minister. With the Minister's approval, the Committee delegated these powers to both the Chairman and the Executive Member. The Committee did not use its powers under section 14 during the reporting period.



## 2.7 Membership of Other Committees and Statutory Bodies

### **Australian Statistics Advisory Council**

The Executive Member, Jacqueline Morgan, is a member of the Australian Statistics Advisory Council (ASAC). The function of the Council is to advise the Treasurer and the Australian Statistician on priorities and programs of work to be adopted in relation to the provision of national statistical services.

The Council's advice to the Australian Bureau of Statistics draws upon the wide spectrum of interests and expertise of its members. Privacy has been recognised as an area requiring particular attention.

Dr. Morgan attended each of the three Council meetings during 1991.

### **Centre for Conflict Resolution**

The Macquarie University established during 1991 a Centre for Conflict Resolution within the School of History, Philosophy and Politics.

The Executive Member, upon invitation, became a member of the Advisory Board of the Centre, and attended the inaugural Board meeting.

### **Consultative Group on the Credit Reporting Code of Conduct**

The Privacy Committee was invited by the Federal Privacy Commissioner to join a Consultative Group for the development of a Code of Conduct on credit reporting, as required by section 18A of the Privacy Act 1988.

The Investigations Officer, Ms. Diane Johnson, represented the Committee at meetings of the Consultative Group throughout 1991.

## **Locating Debtor, Court Case and Other**

A complaint was received that a debt collector had been given access by the Roads and Traffic Authority (RTA) to the complainant's current address.

The Committee advised the complainant that, before September 1989, information regarding date of birth, licence and vehicle registration was made available by the RTA to certain inquirers for a fee. Categories of request included "locating debtor", "court case" and "other". After consultation with the Committee the RTA introduced new arrangements for search of records, which struck out the above categories. Access to this information is now restricted to the following circumstances:

- ★ motor vehicle accident;
- ★ buying a vehicle;
- ★ obtaining a copy of your own traffic record.

The RTA advised the Committee that access to their records by debt collection agencies had ceased in May 1991. In the instant case, as the disclosure of the information had occurred before that date, the access did not breach RTA policy.

## **Refusal to Release Original Medical Records**

The complainant had received treatment at a drug rehabilitation centre and was concerned about medical records relating to his treatment held by the centre. He wanted the files returned to him.

The drug rehabilitation centre advised that they were prepared to make a copy of the file available to the complainant, but were not prepared to release the originals. The centre advised that the files were records of the treatment of a patient and administrative records of the organisation.

The centre indicated that the records were retained for seven years from the time treatment was completed. The records were treated as confidential and third party access was permitted only with the consent of the patient or by requirement of law. The Committee considered the centre's policy to be reasonable and advised the complainant accordingly.

## **Disclosure of Representations on Behalf of Constituents**

A complaint was received from a federal member of parliament claiming that a state government minister followed the practice of disclosing representations made by the federal member on behalf of constituents to the state member of parliament who represented the same electorate as the federal member. The federal member considered the minister's office should handle the representations itself. He argued that as the representations were referred specifically to the minister's office it was the minister's duty to attend to the issue.



The credit reporting agency investigated the complainants' allegations and confirmed that the credit enquiry by the bank was not supported by a credit application. The agency deleted the enquiry from the credit record but was not prepared to put an interpretation on the bank's actions.

The Committee contacted the bank and requested an explanation as to why a credit enquiry on the complainants had been made with the credit reporting agency. The bank informed the Committee that the manager of the branch at the time the enquiry had been made was now retired and was unavailable for comment. A search of the bank's records could find no reference of the complainants ever approaching the bank for a loan.

The Committee considered this complaint to be very serious. The lack of accountability on the part of members of credit reporting agencies has concerned the Committee for many years. In this case, the Committee could do little more than establish that the complainants' allegations appeared to be substantiated and have the entry removed from the credit record.

The Committee is hopeful that the recently introduced amendments to the Commonwealth Privacy Act 1988 will rectify many of the problems that exist under the current system. These amendments, which address credit reporting practices, will come into full operational effect in February 1992.

### Access to Credit Record

The complainants were involved in a legal dispute which had reached the stage of court proceedings. The complainants alleged that a solicitor acting for the other party had placed an enquiry with a credit reporting agency regarding the complainants' credit record.

The Committee was surprised to learn when it requested an explanation from the credit reporting agency that the entry initiated by the solicitor, was in the way of a "professional enquiry". The Committee had never heard of this type of enquiry and was concerned about the effect this type of enquiry may have on a consumer's ability to obtain credit. The credit reporting agency said this type of enquiry would not adversely affect the ability of a consumer to obtain credit. The Committee was not convinced. In the Committee's experience, credit enquiries, not instituted by the subject, are highly likely to have an adverse affect on a credit application, particularly if the subject does not declare the enquiry to a prospective credit provider.

In this instance the credit reporting agency agreed to remove the entry from the complainants' record. The agency also advised that the policy concerning professional enquiries was under review in terms of the fair credit reporting amendments to the Commonwealth Privacy Act.

## Chapter 3

### PROMOTING PRIVACY

#### 3.0 Introduction

Educating the community about why privacy is important and how privacy can best be protected is the Committee's most important task. The Committee endeavours to promote privacy through its contacts with the media, by providing speakers for conferences and seminars and by distributing educational literature such as the Privacy Bulletin and the Committee's reports.

The Committee, too, needs to be educated. It is vital for the Committee to keep informed about developments in technology, policy and the law which may have implications for privacy. The Committee's contact with other privacy and data protection agencies within Australia and throughout the world frequently alerts the Committee to issues which will need to be addressed sooner rather than later.

#### 3.1 Media

The media sought the views of the Privacy Committee on many occasions throughout the year, and the Committee's activities and policies were covered in the press, and on radio and television.

#### 3.2 Speaking Engagements

The Committee is frequently asked to participate in seminars in order to provide the privacy perspective on particular issues. The Committee sees this work as an important aspect of its educative function, and endeavours to meet as many requests as possible. The Chairman and staff members spoke at seminars and meetings on many occasions during the year, including the following:

- ★ Mental Health Review Tribunal, "Privacy and Mental Health Record Systems".
- ★ Department of Medical Genetics, Prince of Wales Hospital, "Genetics and Privacy Issues".
- ★ Current Affairs Study Centre, Conference on the Review of the Privacy Amendment Act 1990, "Is the Act Satisfactory", "Possible Difficulties with the Act and Code".
- ★ Institute for International Research Pty Limited, Conference on Voice Communications, "Privacy Issues with Voice Networks and Databases".
- ★ Institute of Personnel Management Australia Incorporated, "Privacy and Employment".



- ★ New South Wales Society for Computers and the Law, "Privacy Laws Update".
- ★ Public Sector Awareness Week, University of New South Wales, Law School, "Privacy in the Information Age".
- ★ Monash University, School of Banking and Finance, Conference on Privacy in an Information Society, "Reform of Privacy Laws at State Level".
- ★ Law Week 1991, Charles Sturt University, Bathurst, Society for Law and Justice, "Privacy in the 90".
- ★ New South Wales Justices Association, "Privacy in the Information Age".
- ★ Human Genetics Society of Australasia, "Privacy and Genetics".
- ★ Health Informatics Association of New South Wales, "Computerisation of Medical Information".

The Committee also participated in a number of conferences on new developments which resulted in major privacy issues, for example:

- ★ Communications and Media Law Association with the Australian Chapter of the International Institute of Communications. Meeting on Telecommunications.
- ★ 8th International Congress of Human Genetics, Washington, D.C., USA.
- ★ Road Engineering Association of Asia and Australasia (Australian Chapter) - Meeting for Transport Technology Briefing.

### 3.3 Publications

The Committee has produced many reports and publications since its formation.

The publications are distributed to the Parliament, the Attorney General, government departments, private sector organisations and to members of the community.

The Committee continued to receive many requests for its Bulletin, which was published twice during 1991.

A complete list of published reports is provided in Appendix 2 of this Report.

In addition, the Committee has prepared a number of submissions and papers on specific privacy issues. Copies of these submissions and papers may also be made available to the public. Submissions and papers prepared in 1991 included:

The Committee contacted the insurance investigator regarding the allegations. The insurance investigator denied the charge. He stated that the information came directly from the complainant, along with the information which had been declared in his insurance documentation. The complainant counterclaimed that as he did not have full details of his traffic record at that time, he could not have told the investigator at the interview.

The Committee obtained a copy from the insurer of the report prepared by the insurance investigator. The details of the traffic history were the same as the official Roads and Traffic Authority (RTA) record and appeared to support the complainant's allegations. The RTA was unable to determine whether an unauthorised access had taken place, as at the time there was no record kept of accesses made to the database. The RTA has since introduced new procedures which can help identify unauthorised access to the database.

### Mistaken Credit Report

The complainant informed the Committee that he was contacted by another party with a similar name regarding his credit record. Apparently the other party had been declined credit on the basis of the complainant's credit record. The finance company had even provided a hard copy of the record to the other party and he was able to give the complainant full particulars of his financial history.

In explanation the credit reporting agency informed the Committee that the complainant's credit application resulted in an enquiry to the agency, at which time it was found that a credit report existed for a debtor who had similar identity details to the complainant. The credit reporting agency added the complainant's address to the other debtor's file. The file merge was discovered when the complainant contacted the credit reporting agency after he had been refused credit by the credit provider. The agency separated the files and appended a warning notice.

In the Committee's view the credit reporting agency should have taken more care with its matching procedures in this instance. Although there was a similarity in name and date of birth, other personal particulars such as licence number, spouse and address were sufficiently different to alert the agency that further verification with the members who had supplied the particulars would be necessary before a file merge should proceed.

### Confidential Information Disclosed

The complainants were involved in a proposed financial scheme with a solicitor. The proposal was abandoned when the solicitor obtained confidential information concerning their financial affairs. The complainants alleged that their local bank manager had obtained access to their records with the credit reporting agency and disclosed this information to the solicitor.



- ★ 2.0% Media;
- ★ 2.0% Surveys;
- ★ 2.0% Bag Search in Retail Stores.

As noted at 4.5 of this report, during 1991 legislative provisions for credit reporting were introduced as amendments to the Federal Privacy Act with a Code of Conduct being issued in September 1991. A six month adjustment period, to February 1991, was written into the Code to allow credit providers to implement the necessary changes in their procedures.

Credit reporting complaints, following these legislative amendments, will be a federal matter.

#### 6.4 Some Cases

##### **Video Shop Membership**

The complainant asked the Committee's help in having a default entry removed from his credit reporting agency record. A number of years previously, he had joined a video hire shop, then let his membership lapse when he moved to another area. He had no further contact with the video shop and, when he later applied for a loan he was astonished to find that a default report, for a total of \$800, was listed by the video shop on his credit record.

He contacted the collection agency acting for the video shop. He was informed that the default related to two videos that it was claimed he had not returned and to fines due to non return. The complainant strongly denied the claim, but was unable to get the default entry removed.

The Committee contacted the collection agency and requested that the allegations be substantiated. One issue of particular interest to the Committee was whether fines imposed by a video store could properly be considered to be a credit default. As it happened, the Committee did not need to resolve this issue as the collection agency, when it was unable to produce any documentation relating to the dispute, agreed to have the default entry removed from the complainant's record.

##### **Stolen Vehicle Claim**

The complainant alleged that an unauthorised access to his traffic record was made by an insurance investigator assessing his stolen vehicle claim. He stated that at the time of insuring the vehicle he had forgotten some offences and had not declared them to the insurance company. The complainant said that the investigator must obtain information regarding certain infringements from his official traffic record as he had never disclosed them to the insurance company.

- ★ Submission to the Independent Commission Against Corruption "Privacy and Data Protection in New South Wales - A Proposal for Legislation".
- ★ Submission to the National Health and Medical Research Council on Guidelines for the Protection of Privacy in the Conduct of Medical Research.
- ★ Submission to the Federal Privacy Commissioner on the Credit Reporting Draft Code of Conduct.

#### 3.4 Privacy Agencies

During 1991 there were two meetings of Australia's privacy agencies. These meetings are attended by representatives of the Privacy Committee's of New South Wales, South Australian and (until mid 1991) Queensland, of the federal Privacy Commissioner and representatives of government policy bodies in jurisdictions that have yet to enact privacy laws.

The first meeting was held in May in Canberra and was hosted by the Privacy Unit of the Australian Capital Territory. As in previous meetings, each agency presented a report on current activities and developments affecting privacy within their jurisdiction. Agency reports were followed by discussion of privacy and data protection issues of common concern. One of these issues was the proposed Law Enforcement Access Network and a representative of the Commonwealth Attorney-General's Department presented a paper to the meeting about this proposal. The meeting was also addressed by Mr. Greg Tucker, OECD Research fellow in Privacy and Senior Lecturer at Monash University. Mr. Tucker spoke about trends in privacy law in Europe and likely developments in Australia.

The second meeting was hosted by the South Australian Privacy Committee and was held in Adelaide in November. Among the issues discussed at that meeting were:

- ★ the proposed national database of information relating to land ownership;
- ★ access to records held by government agencies to assist in the recovery of debts;
- ★ proposals to extend the telephone interception powers of state and national law enforcement agencies;
- ★ recent developments in drug testing in sport;
- ★ video surveillance of public places for law enforcement purposes.

The meetings also provide a valuable opportunity to exchange ideas about dealing with common privacy problems.



### 3.5 Visitors

The Privacy Committee was pleased to welcome a number of visitors from interstate and overseas including:

- ★ Professor Lance Hoffman, School of Engineering and Applied Science of the Department of Electrical Engineering and Computer Science, The George Washington University, Washington D.C., USA.
- ★ Mark Berthold, Secretary, Law Reform Commission of Hong Kong.
- ★ Greg Tucker, OECD Research Fellow in Privacy and Senior Lecturer, School of Banking and Finance, Monash University, Victoria.
- ★ James Tobin, Vice President, International Consumer Affairs, American Express.
- ★ Tim McBride, Lecturer in Law, University of Auckland, New Zealand.

### 3.6 International Contacts

The Privacy Committee maintains contact with privacy and data protection experts throughout the world. In 1991 this contact was valuable in assisting the Committee to prepare its proposals for new privacy and data protection legislation in New South Wales. The Committee consulted overseas privacy and data protection authorities about the operation of their statutes; the structure and effectiveness of their offices; and their assessment of the relative strengths and weaknesses of their privacy and data protection regimes.

The Committee wishes to place on record its appreciation for the assistance provided by its international colleagues, in particular: the Privacy Commissioner of Canada; the Information and Privacy Commissioner, Ontario; Canada; the Danish Data Protection Agency; the Federal Commissioner for Data Protection, Germany; the Data Protection Commissioner of Hesse, Germany; the Data Protection Commissioner, Ireland; the Registration Chamber of the Netherlands; the Privacy Commissioner, Wanganui Computer Centre, New Zealand; the Department of Justice, New Zealand; the Director of the Norwegian Data Inspectorate; the Swedish Data Inspectorate; and the Data Protection Registrar, United Kingdom.

complainants would not receive further advertising material. The agents said that the particular technology used for compiling and storing the lists did not allow for removal of individual names and addresses. The Committee is undertaking ongoing research on the general issue of access to databases of publicly available personal information.

The following list shows the type and percentages of written complaints received:

- ★ 20% Direct Marketing
- ★ 17% Credit Related;
- ★ 13% Third Party Access to Personal Data;
- ★ 8.0% Employment;
- ★ 5.0% Adoption;
- ★ 5.0% Banks;
- ★ 5.0% Debt Collection Methods;
- ★ 5.0% Police Methods Criminal Records;
- ★ 3.0% Disclosure of Local Council Records;
- ★ 3.0% Media;
- ★ 3.0% Prisons;
- ★ 3.0% Medical;
- ★ 3.0% Surveys and Research;
- ★ 2.0% Insurance AIDS;
- ★ 2.0% Surveillance;
- ★ 2.0% Tenancy;
- ★ 1.0% Roads and Traffic Authority.

During 1991 the Investigations Section introduce a computer statistical record of telephone inquiries received by the Committee. The statistics do not include the category of general privacy or requests for oral advice as well as for Committee publications.

The following list shows the types of telephone complaints received:

- ★ 16.0% Credit Related;
- ★ 13.0% Employment;
- ★ 9.0% Direct marketing Unsolicited Mail;
- ★ 9.0% Surveillance;
- ★ 6.0% Federal Privacy and Taxation Legislation;
- ★ 5.0% Criminal Records Listings;
- ★ 5.0% Debt Collection Methods;
- ★ 5.0% Identifiers;
- ★ 5.0% Insurance Motor Accidents Authority;
- ★ 4.0% Medical;
- ★ 3.0% Adoption;
- ★ 3.0% Banks;
- ★ 3.0% Police;
- ★ 3.0% Neighbours;
- ★ 3.0% Government Records;
- ★ 2.0% Roads and Traffic Authority;



## 6.2 Resolution of Formal Written Complaints

When a complaint is received, the person or body complained of is given details of the complaint and asked to comment on the alleged facts and privacy issues.

Many complaints are resolved at this stage either by explaining the reasons for the action to the complainant, or by making the person complained about aware of the privacy issues and the effect of his or her action. If a complaint cannot be resolved by negotiation between the parties the Committee may prepare a report containing its recommendations regarding the dispute. By giving the report to the parties they are better able to understand the reasons for the Committee's decision, and, as a result, are usually more ready to accept its recommendations.

If the Committee's recommendations are not accepted, the Committee may exercise its discretion to prepare a special report to Parliament.

## 6.3 Statistics

2569 complaints and enquiries were received by the Committee in 1991. Of these, approximately 2424 were dealt with over the telephone.

Files were opened on 148 written complaints and 117 were carried over from previous years.

Files on 104 of these complaints were closed and resolved to the satisfaction of the complainant. Fifty nine were closed where the Committee believed a satisfactory resolution was achieved, even though the complainants remained unsatisfied. Eighteen were found not sustained. A total of 62 files required further research and investigation. In 17 complaints the Committee's recommendation for a policy change was adopted. The Committee's recommendations were not adopted in five cases.

These five cases fell into two categories:

- ★ two files related to requests by former employees for access to specific records held by former private sector employers and one file related to records held by the insurer for a former employer. In all three cases, the files related to medical reports which were now outside time for legal disputation. The Committee recommended that the complainant be given access but in each instance the records were withheld on the stated grounds of legal privilege. The Committee attempted to conciliate these matters, but the employers were not prepared to release the information;
- ★ two files related to requests for names and addresses to be removed from the direct mailing lists of real estate agents. The lists were obtained on microfiche from local councils. In both cases the estate agents claimed that they were unable to amend their own internal lists to ensure the

## Chapter 4

### SIGNIFICANT ISSUES OF 1991

#### 4.0 Introduction

#### 4.1 Independent Commission Against Corruption - Operation Tamba

##### Background

In May 1990, the Independent Commission Against Corruption (ICAC) commenced an investigation into the unauthorised release of information from government records.

The investigation, known as 'Operation Tamba' was prompted by the discovery by police of hundreds of criminal vehicle registration and traffic offence records on the premises of a private inquiry agent. The agent told police that he had paid an anonymous intermediary to obtain the information from a police officer.

It soon emerged that this was not an isolated incident. ICAC uncovered evidence which suggested that private inquiry and commercial agents were routinely obtaining government records for a fee from police officers and employees of the Roads and Traffic Authority, the Department of Social Security and various public utilities. The information was often sought to locate people for debt collection purposes.

There was also evidence of cooperative information exchange arrangements between public officials, banks, real estate agents and others with an interest in locating particular individuals.

ICAC commenced an inquiry into the matter in November 1990 and hearings continued throughout 1991.

ICAC called for submissions from various government departments and authorities concerning their policies and practices in the handling of confidential information.

As the inquiry raised important privacy and data protection issues, ICAC asked the Committee to prepare a submission for its consideration. Issues of particular interest to ICAC included the following:

- ★ What information should and should not be confidential?
- ★ What standards should be imposed on agencies which possess confidential information in terms of their dealing with that information and controlling access to the information?
- ★ Should criminal records, driving and vehicle records be confidential or not?
- ★ If information is to be publicly available, how much information should be made available and for what purposes?



- ★ Should a person seeking information about another person's records be required to establish a bona fide purpose for the inquiry?
- ★ Should a person whose record is the subject of a request be told of the identity of the person who requested the information?

The Committee's submission to ICAC, entitled "Privacy and Data Protection in New South Wales: A Proposal for Legislation", was published in June 1991.

The first half of the submission addresses the specific issues raised by ICAC, referred to above. The other half of the submission sets out the Committee's view of what is required for an effective privacy and data protection regime in New South Wales, namely the enactment of comprehensive legislation and the establishment of an independent supervisory authority.

### **The Recommended Legislative Scheme**

The Committee recommended the enactment of a Privacy and Data Protection Act which includes the following features:

#### Scope and Application

The Act's goal should be the protection of privacy in general, and data protection in particular. It should apply to the public sector but with provision for application to the private sector (either by adoption of the Data Protection Principles or through Codes of Practice).

#### Data Protection Principles

The Data Protection Principles (DPPs) should be the centre-piece of the Act.

The Committee's DPPs are set out in the submission and address the following matters:

- ★ Manner and purpose of collection of personal information;
- ★ Collection of minimum necessary information from the record subject;
- ★ Informed consent to the collection and use of personal information;
- ★ Storage and security of records of personal information;
- ★ Information relating to records of personal information;
- ★ Access to records containing personal information;
- ★ Rectification, notation and erasure of records;
- ★ Use and disposal of records of personal information;
- ★ Limits on use of records of personal information;
- ★ Limits on disclosure of records of personal information.

## **Chapter 6**

### **COMPLAINTS**

#### **6.0 Introduction**

A major statutory function of the Committee is the investigation of complaints. The Committee's complaints function serves four purposes:

1. to resolve complaints;
2. to identify areas where improvements in practices and laws relating to privacy are needed;
3. to draw Committee policy to the attention of those who are breaching privacy; and
4. to provide information which may dispel unjustified fears.

In order to ensure that the Committee's limited resources are allocated fairly and efficiently, the Committee has resolved that, in general, it will decline to investigate complaints in the following circumstances:

1. where the complaint does not relate to privacy;
2. where another body is already investigating the complaint;
3. where another body is available to investigate the complaint and it would be more appropriate for that body to investigate the complaint; or
4. where there is adequate legal redress available to the complainant.

#### **6.1 Resolution of Informal Complaints**

The Committee receives a high volume of telephone enquiries many of which are resolved without the requirement to lodge a written complaint. Approximately 2424 telephone enquiries were received during the year.

People with complaints related to common privacy problems are provided with a statement of Committee policy or an information brochure explaining the steps they may be able to take to resolve the complaint themselves.

A general information brochure has been prepared which includes advice on how to have your name removed from a mailing list, how to obtain a copy of your criminal record, and how to deal with unsolicited telephone calls.



themselves which may involve an interference with the privacy of the person (e.g. through collection of bodily specimens).

A central privacy issue relates to the consent of individuals to medical examinations. Privacy Committee policy requires that the informed and voluntary consent of individuals be obtained before medical examinations occur, unless there is a legal requirement for the examination.

Informed consent means, among other things, that people should be made aware of the specific tests that will be carried out. A general consent to multiple non-specified tests is not informed consent.

People should be made aware of the purposes for which the medical information is sought, including the types of conditions to be detected, and the possible consequences of supplying the information. For example, depending on the result of the health assessment, a person may be refused employment, dismissed, transferred, have their work conditions altered or be subject to ongoing health assessments.

The Privacy Committee is concerned that some occupational health assessment policies support the collection of an unjustifiably wide range of medical and related personal information, in breach of data protection principles. Only the minimum necessary information should be collected.

In October 1990 a report was released by an Interdepartmental Working Party set up to review occupational health services provided by the Medical Examination Centre (now called Health Quest). A new public service policy on occupational health assessments, based on the policies as recommended by the Working Party Report, was being piloted within the Police Service during 1991. It is anticipated that in 1992 new health assessment policies and procedures for application across the public service will be developed based on the pilot study.

The Privacy Committee will continue to consult with Health Quest in 1992 in the development of this new occupational health assessment policy.

As statements of principle, the DPP's are necessarily expressed in broad terms. Since they are minimum standards for general application, broad exemptions to the principles, within the principles themselves, should be avoided. If exemptions need to be made for special cases, these can be accommodated elsewhere in the Act.

The recommended DPPs are set out in Appendix 4 to the Submission.

### Codes of Practice

Instead of wholesale exemptions from the DPPs, Codes of Practice should be used to tailor data protection standards to the activities and needs of different sectors. For example, in the government sphere of operation, Codes could be developed in relation to medical records, medical research, and police records to name a few. In the private sector, industries and organisations could seek codes in relation to particular practices (e.g. direct marketing and debt collection) or particular industries (e.g. insurance, banking and so on).

The Act should make provision for formal endorsement of Codes of Practice by the Commissioner and consideration may need to be given to adopting some procedure to make Codes legally binding (this may be necessary to satisfy international standards).

### Computer Matching and Data Linkage

Programs which involve data matching using the records of more than one agency (either government or non-government) should be reported in advance to the Privacy and Data Protection Commissioner with a statement describing: the type of data to be matched; the source of the data; and the purpose of the match. Notification should not be required if the match has been reported pursuant to the DPPs.

This procedure will ensure greater transparency of information processing practices.

### Transborder Data Flows

The Act should address the issue of transborder data flows by requiring that data should only be transferred out of New South Wales where the transfer is required by law or treaty or where the receiving party can ensure an equivalent level of data protection.

### Enforcement: Offences and Remedies

The Act should create a limited range of offences for the most serious and wilful breaches of data protection principles. Individuals should be able to obtain compensation for damage suffered as a result of the breach of particular data



power to investigate complaints about violations of privacy, would be given the power to investigate complaints about the use and disclosure of information.

The Bill creates a number of specific offences in relation to corrupt dealings with public sector information. For example, current and former public employees would risk a penalty of \$10000 or 2 years imprisonment if they used or disclosed personal information gained in the performance of official functions for the purpose of obtaining a financial or other benefit.

The same penalty would apply to people who attempt to bribe current and former public employees into disclosing personal information; to those who obtain personal information when they ought to have known it was corruptly obtained; and to those who hold themselves out as being able to supply personal information that has been corruptly obtained.

In his Second Reading Speech to Parliament, Mr. Tink described the Bill as a starting point for public discussion. He indicated that the Bill may eventually be considered by a Parliamentary Legislation Committee and may undergo substantial amendment.

There are a number of amendments to the Bill which will be necessary to make it conform with the Committee's proposal for legislation, as outlined in its submission to ICAC. These amendments include provision for the regulation of computer matching and transborder data flows and the establishment of an independent Office of Privacy and Data Protection Commissioner.

The Committee hopes that all its recommendations will be incorporated in the Bill before it is passed. Debate on the Bill is expected to be deferred until the Independent Commission Against Corruption releases its report on Operation Tamba. This report is not likely to be released before mid - 1992

#### 4.3 Privacy and Personnel Records

In 1991, the Department of Industrial Relations, Employment, Training and Further Education (DIRETFE) showed its preparedness to take the lead in matters of privacy policy, by incorporating the Committee's recommended data protection principles into the Public Service Personnel Handbook. From now on, these data protection principles will set the standard to be observed by public sector agencies in dealing with records of personal information, particularly staff records.

The revised Personnel Handbook advises that all records which contain personal information must be dealt with in accordance with the data protection principles. So far as staff records are concerned, public sector agencies are to pay particular attention to the following matters.

##### **Collection of Information**

Only information which is strictly related to employment should be collected.

- ★ A question mark remains over the degree of accountability which will govern access to the system. If the scheme goes ahead, the Committee would favour close monitoring by the Commonwealth Privacy Commissioner. There should be detailed publication of statistics on access in the same way as other forms of intrusion justified on law enforcement grounds (such as telephone intercepts) are reported.

At the end of 1991, the Committee was still monitoring the ongoing development of LEAN which the Commonwealth hopes to have running in the second half of 1992.

#### 5.14 Privacy of Equal Employment Opportunity Data

The Office of the Director of Equal Opportunity in Public Employment (ODEOPE) approached the Committee for guidance on the appropriate data protection standards for the collection and use of equal employment opportunity (EEO) data.

EEO data can include information such as name, date of birth, place of birth, aboriginality, sex, occupation, salary and disabilities. It is collected to ensure that public sector organisations provide equitable access to jobs, career paths and training and equitable conditions of employment for women, Aboriginal people, people of non-English speaking background and people with physical disabilities.

In October 1991, after consulting with the Committee ODEOPE issued "Guidelines for the Protection of Privacy in the Collection and Storage of EEO Group Membership Data". These Guidelines provide detailed instructions to government agencies on how to ensure the privacy and confidentiality of EEO data. A summary of the most important points covered in the Guidelines follows:

##### 1. Voluntary Contribution of Information and Informed Consent

The guidelines stress that staff must be told that their contribution of information about EEO group membership is voluntary. They must also be told what the information is to be used for, who will have to access to it, and what rights they have to access or delete their own information. These data subject rights are conveyed by a cover sheet which accompanies the data collection form.

##### 2. Data Collection

EEO data is to be collected on a separate form from any other application or personnel data form. This helps to ensure that the minimum number of people are involved in handling the data during the collection process.



It also has had the responsibility for developing projects for improved access to the information provided.

The Committee's 1990 Annual Report referred to the proposal for SLIC to set up a Public Enquiry System to market this information electronically and provide a gateway for businesses wishing to access other public and private databases with a land orientation. Reference was made to the Committee's discussion paper which recommended a distinction between appropriate and inappropriate uses of the information to be made available.

To date there has been no firm approval for the Public Enquiry Service. However, SLIC has continued to correspond with the Committee about a number of proposals for access to land information for business purposes. Requests to SLIC for the supply of owner details in electronic form for direct marketing purposes have been turned down in accordance with the Committee's recommendations.

### 5.13 Law Enforcement Access Network

The Committee's 1990 Annual Report referred to concerns about the Law Enforcement Access Network (LEAN). This network proposes to combine state land information and nation-wide company information on a single database where it will be accessible to Commonwealth and State agencies with law enforcement and revenue protection functions.

A pilot project using a sample of land related data taken from New South Wales records (including the Land Information System Hub) was undertaken in the earlier part of 1991. Following evaluation of the pilot scheme a request for tenders was issued towards the end of the year. Documentation associated with the tender process appears to confirm some of the Committee's original concerns, namely:

- ★ Information originally collected to establish the status of particular parcels of land or particular companies will be held in a form in which its main use will be to profile individuals and their assets.
- ★ The searching and matching capacities of the LEAN computer will make it possible to isolate large groups of people who can then become the subject of further investigation (strategic intelligence gathering). This would amount to routine surveillance of significant sections of the population without their knowledge or consent and with no built in legal safeguards.
- ★ Sophisticated searching techniques will be available to departments with routine checking functions. This may tempt some to pry into the affairs of clients and customers without just cause to use these powers to intrude on clients and customers. The large number of terminals with access to the LEAN computer will create opportunities for improper and illicit use.

Where possible the information should be obtained directly from the staff member. If information is to be collected from other sources, the agency should seek the informed consent of the staff member.

### Data Quality

Agencies should not record irrelevant, unsubstantiated, or unvalidated information on staff records.

### Data Security

Agencies should ensure that staff records are reasonably secure from loss, unauthorised access, modification, or other misuse. Attention should be paid to:

1. Physical Security - Filing cabinets should be locked and access to computer records should be controlled. Computer disks should be securely stored. Information on staff records should not be faxed. Records should be sealed before transportation.
2. Organisational Safeguards - Each agency should identify the purposes for which access to staff records may be granted, and the positions within the agency which are authorised to access staff records. Access to records should be graded so that authorised officers are not given access to the full contents of a staff record, unless full access is strictly necessary. If the purpose for which access is sought does not strictly require the disclosure of identifiable information (e.g. compilation of statistics) then only de-identified information should be disclosed.
3. Retention of Records - Staff records should not be retained indefinitely. They should be disposed of in accordance with the General Records Disposal Schedule - Personnel Records 'Issued by the Archives Office of New South Wales'.

### Openness

Agencies should ensure that staff are made aware of the kind of information contained in staff records, who has access to those records and for what purposes.

### Access by Employees

Employees are entitled to have access to their records and may make notes and photocopy information from the record. Photocopies should be permitted on request without cost to the individual. Employees should provide appropriate proof of identity before access is granted.



Employees may nominate a representative to access their record on their behalf. In such cases, access should only be granted with the written consent of the employee.

Access should be given at a mutually convenient time and be supervised to ensure that information is not removed from the file.

### Access by Former Employees

Former employees should be permitted to see their staff records. Photocopies of information on the records should be permitted on request and the agency may charge a fee for providing them.

### Correction of Records

Agencies should make all reasonable corrections, deletions and additions to ensure the information in staff records is relevant, accurate, up-to-date and complete. If an agency declines to amend a record at the staff member's request, he/she should be entitled to attach any statement to the record about the amendment sought.

Where a staff record has been amended, the staff member is entitled to have recipients of the record notified of the alterations by the recordkeeper.

### Adverse Notations

Where any adverse notation or disciplinary action is recorded on a personal file, the person concerned must be shown the notation and permitted to add written comments. The person should be invited to sign the notation, but should he/she decline to do so, no further action is to be taken in this regard other than to record the invitation and the refusal. Agencies should establish independent review committees to review disputed adverse notations and amendments to files.

### Unproved Disciplinary Charge

Where a staff member is found not to have committed a breach of discipline, the charge and any other associated records must not remain on the personal file or any other file and no other record is to be maintained concerning the charge. The charge and all associated records are to be destroyed.

### Use of Staff Records

Generally, staff records may only be used within an agency for purposes specified at the time the information was collected, and by officers with the authority to access these records.

The Commonwealth Privacy Commissioner has put forward draft guidelines on data-matching which provide a process whereby consideration can be given to the privacy issues associated with data-matching and appropriate safeguards can be built in when matching programs are undertaken.

The draft guidelines are intended to be observed by Commonwealth agencies proposing to carry out data-matching programs, including those programs using information obtained from other bodies and organisations, (e.g. state authorities like the MAA).

The collection and use of a certain amount of information from the MAA claims register is authorised by law under the Social Security Act 1991. However, at least until the Commonwealth data-matching guidelines are issued, the Committee considered that it is doubtful that sufficient safeguards existed to ensure:

- ★ that the data-matching using MAA information is justified by substantial social benefits that outweigh the privacy interests of the individuals concerned;
- ★ that any data-matching program is conducted in a manner which avoids any further and unnecessary intrusion into privacy and avoids unfairness.

The Privacy Committee recommended that the DSS postpone this data-matching program at least until the proposed Commonwealth data-matching guidelines are in place and that, if the DSS resolved to continue with the program, public notice of the program should be given and data subjects should be informed of the disclosure of their personal information. The DSS declined to accept the Committee's recommendations.

### 5.12 State Land Information Council

The Committee continued to monitor the privacy implications of the computerisation of land information systems during 1991. Because of Australia's comparatively high rate of home-ownership, land information provides an attractive reference source for direct marketers and other organisations with an interest in having up to date addresses and ownership details. It is also attracting the interest of government agencies.

In New South Wales, land ownership details are recorded in a public register, which anyone can inspect to confirm who owns a particular block of land. Further information is collected by public authorities at the time of a purchase for rating and valuation purposes. With computerisation it has become possible to combine all of this information for easy retrieval and access. The resulting exposure of large amounts of personal information poses a threat to privacy.

The State Land Information Council (SLIC) was set up to coordinate the various sources of information. It currently operates a Land Information System Hub which collects and checks the information received from different departments.



### 5.11 Commonwealth Data-matching Using State Records

In October 1991, the Privacy Committee was approached by the Motor Accidents Authority (MAA) for advice about a request it had received from the Department of Social Security (DSS) for information from the Motor Accidents Authority claims register.

The MAA is a New South Wales statutory body established under the State compulsory Motor Accidents Act 1988 (NSW) and it maintains a register of motor accident insurance claims made under the third party insurance scheme.

The MAA advised the Committee that the DSS wished to obtain a computerised file containing information on all people who had received insurance payments within the last 12 months and whose details were recorded on the MAA claims register.

In respect of each such person, the information requested comprised:

- (a) full name and any previous name;
- (b) address;
- (c) sex;
- (d) date of birth;
- (e) date of death;
- (f) any payments received by the person from an insurer.

The MAA information was intended to be used in a data-matching program to identify persons who have received insurance payments which may affect their eligibility for pensions, benefits or allowances under the Social Security Act 1991.

In effect, the MAA was being asked to disclose information about all people who had received compensation payments. Clearly, this group would include people who had never claimed benefits from the DSS and who had never had any contact with the Department.

The DSS has extensive statutory powers to require individuals and public and private sector agencies to provide it with information about individuals and classes of persons. Notwithstanding the fact that, in this case, the DSS had the legal authority to require MAA to comply with its request, the Committee was concerned that the data matching exercise would infringe the privacy rights of insurance claimants. It is clearly contrary to data protection principles for information collected for one purpose (e.g. processing of insurance claims) to be used for a completely different purpose (e.g. eligibility for welfare benefits) without the knowledge and consent of the data subject.

Data-matching is an investigative technique which frequently involves the systematic breach of an individual's information privacy rights in that personal information is used for purposes other than those for which it was collected and the data subject is not made aware that the data match will be conducted.

The informed consent of the record subject should be obtained before any other use of a staff record is made.

### **Disclosure of Staff Records Outside the Agency**

Information from staff records should only be disclosed outside the agency:

- ★ where the consent of the record subject has been obtained;
- ★ to prevent or lessen a threat to the life or health of a person; or
- ★ by requirement or authority of law.

A record should be maintained of each access to the record showing the identity of the person who obtained access and the reason access was granted. This record should be made available to the employee on request.

### **Provision of Staff Records to Workers Compensation Insurers**

Disclosure of information from staff records to workers compensation insurers is an example of where disclosure is required by law.

Section 93(1)(b) of the Workers Compensation Act 1987 requires an employer who receives a request from the insurer for information in respect of a claim, to furnish the insurer with such specified information as is in the employer's possession or reasonably obtainable by the employer, within 7 days.

Agencies are encouraged to inform staff when access to their file is sought by an insurer and advised them how much information is to be disclosed.

## 4.4 Criminal Records Act

The Committee has consistently advocated the need for spent conviction legislation to address the issue of old criminal records. The Criminal Record Act proclaimed on 31st May 1991 was a welcome step, though one which did not go as far as the Committee would have hoped.

The object of the Criminal Records Act is to limit the effect of a person's conviction for a relatively minor offence, provided that the person completes a minimum period of crime free behaviour. For adults the crime free period is ten years from the date of conviction and for child offenders the period is reduced to three years.

Some convictions are incapable of becoming spent. These are:

- ★ convictions for which a prison sentence of more than 6 months has been imposed;



- ★ the failure to provide for notification of individuals when their credit information has been disclosed to another party in error;
- ★ the Privacy Commissioner's determination of the definition of "credit providers" which has increased the number of organisations that can be permitted access to credit information files under the legislation;
- ★ credit providers reporting cases of simple overdue payment as "serious credit infringements", thus circumventing the general 60 day waiting period before overdue payments can be reported.

#### 4.6 Privacy Law Reform in Other States

##### Queensland

Until recently, the Queensland Privacy Committee had the responsibility for the oversight of privacy issues in that state. On 14th June 1991, however, the Privacy Committee Act 1984 (QLD) expired and at the time this report was written, a replacement body had yet been appointed.

Before the Privacy Committee was disbanded, it put forward a number of recommendations, including the following:

- ★ the Invasion of Privacy Act should be amended and strengthened to ensure data is used only for the purposes for which it is gathered; to provide for the licensing of data gatherers such as private investigators; to establish rights in relation to freedom from surveillance and harassment; and to provide for limited court based sanctions and remedies such as fines, restraining orders and damages;
- ★ a new Privacy Committee should be established, consisting of representatives of the public and private sectors. Members should be appointed by the Minister;
- ★ a number of matters should be referred to the Law Reform Commission for consideration including powers of search and seizure and publicity given to criminal proceedings.

Also during 1991, Queensland's Minister for Justice and Corrective Services released a discussion paper concerning the establishment of a new privacy body for Queensland.

The Discussion Paper proposed that a new privacy body be set up which combines the features of the Office of the Federal Privacy Commissioner and the New South Wales Privacy Committee.

The new body would closely resemble the New South Wales Privacy Committee in jurisdiction and functions, but its executive member would be called the Privacy Commissioner. The privacy body would use the OECD Guidelines

criminal record information), about individuals connected with casino operations.

The Committee advised that, in accordance with data protection principles, the investigating bodies should ensure that people subject to investigation and inquiry give informed consent to the required checks. The need for openness in information collection means that, as far as possible, people should be made aware of the information sources that the investigating bodies may consult.

The consent of other people connected with the primary subject of investigation should also be sought if they, in turn, are to be subject to inquiries. These other people might include family members, friends, and business associates.

As investigations and inquiries may result in the collection of a considerable quantity of sensitive personal information it is particularly important that adequate procedures be developed in relation to the security and retention of the information. The Committee also advised that details of rejected applicants' records should be destroyed when no longer required.

Further privacy issues were raised by proposals for optical surveillance. The draft Bill anticipated the implementation of procedures for the use and maintenance of security and surveillance facilities including catwalk systems and closed circuit television systems.

The Committee advised that any security and surveillance facility should only be used for specific, defined purposes related to security and not for building profiles of the gambling activities of identified casino patrons or other secondary business or research related purposes. If records of casino patrons are collected through surveillance, for example on video-tapes, procedures should be implemented for the security and destruction of these records once they are no longer required.

The Committee also advised that patrons of casinos should be notified they may be subject to surveillance while in the casino.

#### 5.8 Disclosure of Registry of Births, Deaths and Marriages Information to the Australian Institute of Health

The Privacy Committee was asked by the New South Wales Registry of Births, Deaths and Marriages to advise on a proposal that the Registry provide death index and death register information to the Australian Institute of Health for the purposes of establishing a National Death Index.

The stated aim of the National Death Index is to assist in the undertaking of epidemiological studies, both by the Institute directly and by other medical researchers.



The Privacy Committee advised that it opposed the Social Issues Committee's recommendation that in all cases where minors are issued with infringement notices their parents or guardians must be informed.

However, the Committee also advised that it would not object to parents being notified as an exercise of Police discretion, especially in the case of offenders under the age of 16, provided that the discretion to notify the parents is exercised by the senior officers responsible for administering juvenile cautions.

## 5.6 Disclosure of Student Results to Residential Colleges of the University of Sydney

The Privacy Committee responded to a request for advice from the University of Sydney on proposed policies to be followed by the University in relation to disclosure of student academic results.

It is Privacy Committee policy, and an important data protection principle, that personal information should not generally be disclosed without the consent of the individual to whom it relates.

The University suggested the implementation of a policy that would allow the disclosure to Colleges of the marks and grades of students in residence at Colleges only where individual students provided written consent as part of their College registration.

The Privacy Committee agreed that the disclosure of this information should only occur with the informed consent of the individual College students. Informed consent would also mean that the students should be aware of the effect on them, if any, of not agreeing to the disclosure of their results to the College.

## 5.7 Casino Inquiry

The Privacy Committee was asked to comment on matters being considered by the Inquiry into the Establishment and Operation of Legal Casinos and in particular on the draft Casino Control Bill 1991.

One of the stated aims of the legislation is to ensure that the management and operation of casinos remain free from criminal influence and exploitation.

The draft Bill sets up criteria and procedures for the granting of licences to operate casinos and for the licensing of certain classes of casino employees and persons who have a special relationship with a casino. The provisions of the draft Bill require investigations and inquiries about these licence applicants, and about persons engaged in the administration of the casino legislation.

The various vetting processes would involve the collection of a wide range of personal information, some which may be extremely sensitive (for example

on the Protection of Privacy (1981) to guide its deliberations on information privacy issues and these Guidelines would be incorporated in the legislation.

At the end of the reporting period the issue was still under consideration by the Queensland Government.

## South Australia

In late 1990, the South Australian Parliament established a Select Committee to consider any deficiencies in the law relating to privacy. In particular, the Committee was asked:

- ★ to consider a private member's draft privacy bill;
- ★ to examine and make recommendations about specific areas where privacy protection is needed.

The Select Committee reported during 1991 that, in its view, a new law was necessary to create a general right of privacy. It proposed a number of amendments to the existing Privacy Bill and this Bill was subsequently considered and amended by the Legislative Assembly.

The Privacy Bill 1991 establishes a statutory tort of privacy. Certain activities, such as intruding on another's personal or business affairs by keeping them under observation will give rise to an action if infringement is substantial and unreasonable and not justified in the public interest. The remedies available under the Bill are damages and injunctions, but injunctive relief may not be granted against a media organisation.

The exemptions to the Bill are very generous; individuals and organisations exempt from the Bill include members of the police force, other people vested with statutory powers of investigation or inquiry, insurers and commercial organisations trying to detect fraud and debt collectors.

The Bill also establishes wide grounds for defence against an action for infringement of privacy. These include the defence that the infringement was necessary for, or reasonably incidental to the protection of the "lawful interests" of the defendant. Where the defendant is a media organisation, it can claim the defence that the privacy intrusive action was in accordance with guidelines adopted by the Australian Journalists Association or the Australian Press Council.

The Bill does not directly address data protection. Instead, it gives the Governor the power to make regulations laying down standards of privacy for organisations that keep records relevant to the personal or business affairs of others.

At the end of 1991, the Bill had not been passed by the South Australian Parliament.



## Chapter 5

## ADVICE

5.0 Introduction

The Privacy Committee Act 1975 empowers the Committee to: 'make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons' (section 15(1)(c)).

The majority of the Committee's reports and recommendations arise out of requests for advice. Each year, the Committee receives a large number of requests for advice from local, State and Commonwealth government agencies, community groups, unions, business and professional associations, legal and medical practitioners, universities, technical colleges and other educational institutions as well as from various agencies in other countries and from members of the public.

The Committee does not always wait until a request is received before it offers its advice. From time to time, a media announcement or complaint will alert the Committee to a matter that requires immediate attention. In such cases, the Committee will approach the organisation or individual concerned and seek further information about the matter so that appropriate recommendations can be made.

During 1991, the Committee opened files on 293 requests for advice. This may be compared with 273 requests in the previous year.

Most of the requests for advice (59%) came from local, state and Commonwealth government authorities, 30% came from the private sector and the remaining 11% from schools, technical colleges and universities.

The Committee's research staff spend considerable time and effort reviewing and researching policies and administrative procedures of various public and private organisations in order to develop appropriate recommendations and guidelines.

Some examples of the Committee's advisory work are set out in this Chapter.

5.1 "Outing" Policy Statement

In August 1991 controversy arose in relation to threats by gay activists to publicise the names of prominent people who were claimed to be homosexual.

The controversy led to the Privacy Committee adopting the following policy statement on the practice of "outing":

The Privacy Committee strongly advised the RTA to review the operation of the police report procedure. The Committee suggested that a less privacy invasive means of assessing licence applicants would be through a questionnaire procedure. A questionnaire could require the licence applicant to answer questions relating to drinking and or driving habits. The questionnaire could be administered by the police or self-administered by the applicant, perhaps in the form of a statutory declaration.

In relation to the existing police report procedure the Privacy Committee also recommended that:

- ★ a copy of the police report should be supplied to the licence applicant;
- ★ the RTA should indicate clearly to police officers that only information relating to convictions for specified categories of relevant offences is being requested.

5.5 Underage Drinking Infringement Notices

The Chief Secretary requested the Privacy Committee's advice in relation to the infringement notice scheme for underage drinking offences. The Committee was asked, in particular, to comment on the recommendation of the Social Issues Committee of the Legislative Council that in all cases in which minors are issued with infringement notices their parents or guardians must be informed.

The Committee considered this matter at length and agreed with the Social Issues Committee that the problem of underage drinking is a serious one, both for young people and for society at large. The Committee also recognised that parents have a primary responsibility to give appropriate guidance to young people on responsible attitudes to drinking and adherence to the law.

However, the Committee considers that young people, especially those approaching the age of 18, have the right to a degree of privacy and personal autonomy independent of their parents or guardians.

If young people are entitled to a right to privacy then disclosure of information about them to their parents, without their prior agreement, is a breach of a widely accepted data protection principle. This principle states that, in general, recordkeepers should not disclose personal information to a third party unless the individual concerned has consented to the disclosure or the disclosure is required by law.

The fact that notification of parents and guardians is not practised in the case of similar offences under the Summary Offences Act and traffic legislation and that the police service identified practical difficulties in notifying parents were also seen as relevant to the Committee's consideration of this matter.



- ★ there would be limitations on the conviction or charge information which was disclosed (no information would be given on offences over 5 years old, with the exception of assault and sexual offences);
- ★ the results of the check would be discussed with the subject before any adverse decision is made.

The Committee recommended that the draft guidelines be clarified to ensure that checks were only carried out on successful applicants for positions. It also noted that the nature of the specified positions made it appropriate that the five year limit not apply in relation to sexual offences.

#### 5.4 Police Reports on Applicants for Drivers' Licences

A magistrate asked the Privacy Committee to consider whether procedures used by the Roads and Traffic Authority (RTA) to assess whether drivers who have had their licences cancelled for drink driving offences should have their licenses renewed are unjustifiably privacy invasive. In particular, the Committee was asked to examine the use of police reports about licence applicants which are requested by RTA..

It is a principle of information privacy that personal information should only be collected when it is relevant to the decision being made. In addition the information collected should be accurate, up to date and complete.

The police reports requested by the RTA ask police to assess whether a person is of "sober habits". The Committee was concerned that there appeared to be no definition of what constitutes "sober habits" to guide police in making this assessment. In any case, the ability of police officers to assess reliably whether or not a person is of "sober habits" is open to doubt.

Other questions on the police report forms raised related privacy concerns. One question asked police whether there are "any incidents, other charges or offences involving the person, recorded at the local Police Station". The RTA agreed that only information about convictions for traffic or drug alcohol related offences was relevant to the licensing procedure. However the way the question was framed invited the disclosure of other information. The Committee is aware of at least one occasion on which this question resulted in the disclosure of information on irrelevant offences and dismissed charges.

A further concern noted by the Committee was that it is not RTA policy to give copies of the completed police report to the licence applicant. Where information is collected from a third party and is sufficiently adverse to affect a decision against a person's interests the content of the information should be communicated to the person prior to an adverse decision being made. Privacy Committee policy provides that government bodies receiving police reports should, wherever possible, provide a copy to the persons affected so they can check the accuracy of the report.

*"Outing" is a term currently being used to describe the practice of publicly disclosing the concealed sexual preferences of a person.*

*The Privacy Committee believes that information about the sexual orientation and behaviour of a person is personal information of great sensitivity.*

*Disclosure of information on these matters without the consent of the person constitutes an invasion of privacy. The Privacy Committee condemns this practice.*

#### 5.2 Video Surveillance of Public Places by Police

In the past the size, cost and technical requirements of cameras limited their effectiveness and usefulness for surveillance. However, camera and video equipment is getting smaller, cheaper and easier to operate. There is already significant use of video surveillance in public places, such as in bank foyers and in retail stores so it is hardly surprising that police are interested in using video surveillance for the prevention and investigation of crime.

In March 1991 the Committee received a request for advice from a police patrol about a proposal to install video surveillance equipment at several locations within the patrol district. The locations included two council carparks and a public park.

##### **Privacy Issues**

The Privacy Committee considers video surveillance to be inherently privacy invasive. Electronic visual surveillance by government, more than any other form of electronic surveillance, reminds people of the spectre of Big Brother watching at all times and in all places. It has been said that the totalitarian government depends on secrecy for the state and intensive surveillance of its citizens. The democratic state relies on publicity of its actions, and on privacy of its people.

Video surveillance involves the collection of information about and the observation of, law abiding citizens. It involves the systematic observation of people without any suspicion of wrongdoing and the observation of activities unrelated to those being watched for. For these reasons video surveillance can have an adverse effect on civil liberties including the freedom of association, assembly and travel.

The "chilling" effect of surveillance on the exercise of civil liberties has been widely noted. When people know they are being watched (and especially if they know they are being recorded) they may restrict even quite lawful actions, in case those carrying out the surveillance may suspect them of some wrongdoing if they behave at all "abnormally".



Under the proposal, considered in detail by the Privacy Committee, members of the public leaving the council carparks or entering the public park would be videotaped. Since video surveillance is privacy invasive there needs to be a strong social justification for its use. The Privacy Committee was not convinced that in this case such a justification had been established.

In reaching this conclusion the Committee looked at the nature and extent of problems the video surveillance was intended to address. These problems included motor vehicle theft and dumping of stolen vehicles. The Committee also studied the alternative, less privacy invasive measures which exist for dealing with these problems, such as controlling access to carparks, employing security guards and encouraging better security by car owners.

The Privacy Committee advised the Police that it opposed the introduction of the proposed video surveillance. At the end of the reporting period the video surveillance systems had not been introduced.

### 5.3 Criminal Record Checks

In May 1989, following consultation with the Committee, guidelines for Criminal Record Checks were issued by the Government Recruitment Agency within the Department of Industrial Relations and Employment (DIRE). These guidelines have now been incorporated in the current Public Service Personnel Handbook.

The Guidelines provide that pre-employment criminal record checks in the public sector should only be conducted for "sensitive" positions and the checks should be limited so as not to disclose:

- ★ offences over five years old except where a person has been in prison during the five year period;
- ★ charges dismissed, successfully appealed against or adjourned;
- ★ charges which have been dealt with without conviction and where any recognizance has expired; and
- ★ juvenile offences.

Where charges or appeals are still pending, a final decision should be deferred where possible, the applicant should be appointed on probation, or given preference for the next suitable vacancy if acquitted.

#### **Criminal Record Checks for School Based Positions**

The Department of School Education recruits staff to a range of "sensitive" positions involving direct contact with children. With the Privacy Committee's approval more rigorous checks are conducted on staff appointed to teaching

positions than the Guidelines would otherwise allow, particularly in the case of offences which may be relevant to risks of child sexual assault.

In June 1991 the Committee was asked to approve a request from the Department for wider criminal record checks to be conducted on applicants for non-teaching positions which involve contact with children. It was proposed to check for sexual offences whenever they occurred and all convictions for other offences occurring within the last ten years.

The Committee considered the Department's request and advised that it had no objection to the Department obtaining records of:

- ★ all convictions of sexual offences no matter how long ago they occurred;
- ★ all child sexual assault charges dealt with under Section 556A of the Crimes Act (case proved but discharged without conviction);
- ★ any child sexual assault charge dealt with through a pre-trial diversion program (applicable to such offences where offenders are minors).

However, the Committee was not prepared to give blanket agreement to the Department obtaining records of convictions for non-sexual offences outside the five year period provided for under the Guidelines.

The Committee advised that information on pending charges in relation to both teaching and non-teaching positions which have still to be heard at the point of selection should not be obtained, except in the case of sexual offences.

In making its recommendation the Committee was mindful of the need for public sector employers to stay within the Guidelines unless they can make out a case justifying a specific exemption. Such a case was established in relation to concern over sexual assault but no material was offered to justify a departure in relation to other kinds of offences.

#### **Child Care Workers**

Access to criminal record checks for non-government employment is strictly limited. In 1991, the Department of Community Services proposed to extend criminal record checks to private sector child-care workers. Checks were to be undertaken on all licensees and authorized supervisors of care centres, all home-based child care providers (including foster parents and other adults living with them) and all Family Day Care co-ordinators.

The Committee approved searches being conducted in accordance with draft guidelines submitted by the Department provided that appropriate legislative authority existed. The draft guidelines ensured that:

- ★ there would be no criminal record checking carried out without the knowledge of the subject;



*P. Hamilton*



## PRIVACY COMMITTEE

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

# **Survey Guidelines: Guidelines for Surveys and Research**

**No. 42, (Revised), NOVEMBER, 1979**

(See also Research and Confidential Data:  
Guidelines for Access—No. 35, September, 1978)



Colour of Folder - Yellow

*Green*

GUIDELINES PUBLISHED BY THE COMMITTEE  
TO AID IN THE CONDUCT OF SURVEYS AND  
RESEARCH

BP42 (Revised) November 1979



## FOREWORD

In January, 1978, the Committee issued an exposure draft "Guidelines for Surveys" (BP42).

Copies of the draft were widely circulated and many comments and suggestions were received. These led to further discussions and research. In addition, the Committee's complaints' experience assisted it to understand the privacy issues involved.

U { The Committee believes that the development and maintenance of adequate ethical standards by relevant professional and industry bodies are important. Public confidence depends considerably on professionals setting and maintaining appropriate standards of behaviour. Undoubtedly, conflicts will arise between different interests. In general, these should be resolved in favour of the public's interest. U

X The Committee received considerable assistance in developing these guidelines from the International Code of Marketing and Social Research Practices published by the International Chamber of Commerce in 1977. This Code has been adopted by the Market Research Society of Australia as well as a number of other bodies set out in Appendices I and II to this paper. The Committee believes that this Code should be read in conjunction with its guidelines as far as market research is concerned.

The Committee would like to express its appreciation for the assistance given by bodies listed in Appendix 1 in the development of these guidelines. Naturally, individual practices will require appropriate adaptation of the guidelines. The guidelines are flexible enough to permit this.

The Committee believes that if these guidelines are implemented in a spirit of professional and ethical concern for privacy, not only will the interests of the public be served, but also better research will result.

V Experience has shown that if due regard is had to the effects on privacy of surveys and problem areas avoided, both response rates and the quality of data will improve.



# C O N T E N T S

	<u>Page</u>
1. <u>INTRODUCTION</u> . . . . .	1
1.1 Background . . . . .	1
1.2 Surveys and Privacy . . . . .	1
1.3 Surveys and Ethics . . . . .	2
1.4 Explanation of Terms . . . . .	2
2. <u>THE GUIDELINES</u> . . . . .	4
2.1 <u>Finding Potential Informants</u> . . . . .	4
2.1.1 <u>Recognise the Special Sensitivity of Pre-Identified Approaches</u> . . . . .	4
2.1.2 Take Care with Unidentified Approaches . . . . .	5
2.2 <u>Contacting Potential Informants</u> . . . . .	6
2.2.1 <u>Recognise the Possible Inconvenience of Approach</u> . . . . .	6
2.2.2 Include a Frank and Adequate Introduction . . . . .	7
2.2.3 Identify the Interviewer . . . . .	7
2.2.4 Avoid Pressure, Especially with Children, the Elderly and Migrants . . . . .	8
2.2.5 Gain the Informant's Consent to Proceed . . . . .	8
2.2.6 Give Adequate Warning of Use of Recording Devices and Observation Mirrors . . . . .	9
2.3 <u>Collecting Information from Informants</u> . . . . .	9
2.3.1 <u>Only Identify Informants where there is a Particular Need</u> . . . . .	10
2.3.2 Tell Informants of any Indirect Identification . . . . .	10
2.3.3 Answer an Informant's Questions Truthfully . . . . .	11
2.3.4 Respect an Informant's Request to Vary Consent . . . . .	12
2.3.5 Avoid Abuse of the Survey Relationship . . . . .	13
2.4 <u>Processing of Data and Publication of Results</u> . . . . .	13
2.4.1 <u>De-Identify Data as soon as Need has Expired</u> . . . . .	14
2.4.2 Limit Uses of Identified Responses . . . . .	14
2.4.3 Restrict Dissemination of Identified Responses . . . . .	15
2.5 <u>Compulsory Surveys: Variations to these Guidelines</u> . . . . .	16
3. <u>APPENDIX I - List of Relevant Bodies</u> . . . . .	17
4. <u>APPENDIX II - International Code of Marketing and Social Research Practices Published by the International Chamber of Commerce in 1977</u> . . . . .	18 - 27



## 1. INTRODUCTION

### 1.1 Background

This paper deals with privacy issues arising from surveys carried out by organisations and individual researchers. The Committee's experience with surveys stems from two sources: (1) complaints about intrusive surveys from members of the public, and (2) advice sought from the Committee by surveyors wishing to respect people's privacy. On the basis of this experience, the Committee has drafted the guidelines in this paper. In fact, this document in its exposure draft form has already gained wide acceptance and day to day use, both by surveyors and the Committee itself. Where appropriate, readers should also consult the Committee's Background Papers 26 (on Unsolicited Mail and Leaflets), 29 (on Unsolicited Telephone Calls), 31 (Guidelines for the Operation of Personal Data Systems) and 35 (Research and Confidential Data: Guidelines for Access).

### 1.2 Surveys and Privacy

There is no doubt that many surveys serve valuable purposes. For example they can enable:

- manufacturers and retailers to understand what products different types of consumers do and do not want;
- government planners to provide the sort of social, educational, health and transport facilities the community wants;
- members of local, state and federal government to understand current attitudes of their constituents to particular issues;
- medical researchers to discover correlations between particular illnesses and people with particular characteristics or habits.

There is also no doubt that some surveys cause some people concern that their privacy is being unduly invaded. Some people may object to the initial contact if it is unsolicited. Others may object to or fear the collection of information about them, its uses and the possibility of subsequent dissemination. On the other hand, it is recognised that some people enjoy participation in a survey and are unconcerned about privacy.

Because neither the amount of information needed by society nor the degree of privacy to which the individual is entitled is absolute, some individuals will continue to fear that their privacy is being invaded at a time when others will remain quite unconcerned.

The extent of intrusion must be weighed against the benefit to the surveyor and ultimately to the community.

In the Committee's experience, privacy concerns are greatly diminished where:-

1. the survey is voluntary and clearly stated to be so to the informant; and
2. the informant is not identified, or, where he is, the reasons for such identification are explained to him.



The Committee believes that in the great majority of instances the objectives of surveys can be achieved without undue intrusion into individual privacy and without creating undue fears amongst the community. This paper is an attempt to provide guidance to surveyors as to how they may do this.

### 1.3 Surveys and Ethics

The Committee believes that the development and maintenance of adequate ethical standards by relevant professional or industry bodies is important. Public confidence depends considerably on professionals setting and maintaining appropriate standards of behaviour. Undoubtedly, conflicts will arise between different interests. In general these should be resolved in the interests of the public.

See the appendix (p.17) for a list of relevant professional and industry bodies.

### 1.4 Explanation of Terms

In this paper:

- (a) Survey means the systematic collection and recording, classification, analysis and representation of data concerning the behaviour, characteristics, needs, attitudes, opinions, factual details, physical state, etc. of individuals and organisations within a prescribed context. A survey may involve market, social, medical, government or pure research.
- (b) Surveyor means any individual, company, group, public or private institution, etc. which directly or indirectly conducts or acts as a consultant in respect of a survey project or offers its services to do so. An interviewer is generally the agent or representative of the surveyor who personally conducts the interview.
- (c) Client means any individual, company, group, public or private institution, etc. (whether or not such client belongs to the same body as the researcher) which commissions, requests, authorises, or agrees to subscribe to a survey project or proposes to do so.
- (d) Informant means any individual, group or organisation from whom any information is sought by the surveyor for the purposes of a survey project, regardless of the type of information sought or the method or technique used to obtain it. The term informant therefore covers not only cases where information is obtained by verbal or questionnaire processes but also cases where other methods such as observation, postal surveys, mechanical, electrical or other recording equipment are used.
- (e) Interview means any form of direct or indirect contact (including observation, electro-mechanical techniques, etc.) with informants, the result of which is the acquisition of data or information which could be used in whole or in part for the purposes of a given survey project.



- (f) Record(s) means any questionnaire, observation notes, audio or audio-visual recording or film, tabulation or computer print-out, EDP tape or other storage medium, formula, diagram, report, etc. in whatever form, in respect of any survey project.



## 2. THE GUIDELINES

### 2.1 Finding Potential Informants

There are several ways of finding or selecting potential informants for participation in a survey. The method chosen often depends on the nature of the survey. Where a particular identified person is sought (according to the surveyor's prior knowledge of that person's name or other identifiable characteristics) this is categorised as a pre-identified approach. On the other hand, an unidentified approach is one to a person who is unknown to the surveyor.

#### GUIDELINE (1)

*A person should be able to exercise his own control against all approaches, whether pre-identified or unidentified. The surveyor should recognise and respect the exercise of that control.*

*With respect to pre-identified approaches, the surveyor should make clear to the informant what was the source of his identity when asked. Public lists are generally not a problem. However, with private lists, the more unrelated the source list is to the survey, the greater is the need for clarity in communication by the surveyor.*

*With respect to unidentified approaches, while these are generally not a problem, the surveyor should recognise and respect a person's exercise of control against this type of approach.*

#### 2.1.1 Recognise the Special Sensitivity of Pre-Identified Approaches (known by name to the surveyor prior to the approach)

Examples of pre-identified approaches and the Committee's comments on each one are as follows:-

##### (a) From a Public List

Two major "public lists" appear to be particularly relevant. They are the Electoral Roll and the telephone directory.

- (i) The Electoral Roll exists basically to permit the orderly running of elections. The list must be accessible to the public in order to make effective the right to challenge any unregistered voter's right to vote. Due to the list's public availability, and its substantial coverage of the adult population, additional uses have developed, including sourcing of potential survey informants. The Committee does not object to this use. See the Committee's background paper on the Electoral Office (BP38).
- (ii) The Telephone Directory is the other relevant "public list". The privacy issue here is that some private telephone subscribers may presume that their listing in the directory should not be available for unsolicited calls. The Committee is researching this question so as to provide adequate protection for those subscribers who feel that way. Meanwhile, the Committee does not object to this use. See the Committee's background paper on Unsolicited Telephone Calls (BP29).



(b) From a Private List

The Committee foresees four categories of private list:

- (i) A commercial mailing list is a privately compiled list which is often extracted by category from either the above two lists or the organisation's own customer lists. These extracts have been known to be matched for even finer tuning. For instance, an organisation may wish to survey residents of a particular electoral district, but excluding its own credit customers, and can do this by matching the two relevant lists. The Committee does not object to these lists per se. Its views are contingent on the type of private list used as input to create the matchings (see comments below).
- (ii) A related private list such as the surveyor's or client's own customers or clients. This is a frequent use by market research organisations and is not objected to by the Committee as long as these private lists are in general only used where the survey's aims are, or are closely related to, a purpose for which the data was originally collected. For example, a shipping line should be able to approach by itself or commission a surveyor to approach former passengers as to their reactions to their voyage or related matters.
- (iii) An unrelated private list of another organisation (unrelated to the surveyor or client) which has been made available to the surveyor. The Committee feels that this method is not desirable unless the possibility of a survey was clearly in the mind of the data subject when he provided the record keeper organisation with source data about himself. The next alternative, (iv), is much preferred.
- (iv) An unrelated private list of another organisation where that organisation makes the approach on behalf of the surveyor. This is acceptable where the survey's aims are, or are closely related to, the purpose for which the data was originally collected. An example would be a hospital approaching ex-patients who had been treated for a particular problem, to ask whether they would be prepared to take part in a survey by a medical research organisation unconnected with that particular hospital.

2.1.2 Take Care With Unidentified Approaches (not known by name to the surveyor prior to the approach)

Examples of unidentified approaches are:

- (a) to a home, by doorknock;
- (b) to a home, by leaflet;
- (c) to a person in a public place, usually by stopping passers-by;



- (d) to a person by public invitation, either through the media or club and society newsletters; and
- (e) to a person at his place of work.

The Committee has no objections to unidentified approaches, subject to the following comments.

The Committee believes that while freedom of speech should be balanced with privacy interests, a person should be able to exercise his own control against this type of approach. The surveyor should recognise and respect the exercise of that control. The Committee has received complaints where the surveyor has ignored the person's attempted exercise of control. In both of the following examples, the surveyor agreed to instruct its interviewers to recognise and respect the wishes of potential informants:

- (1) The surveyor disregarded an up-to-date "No Hawkers or Canvassers" sign. The Committee regards an up-to-date "No Hawkers or Canvassers" sign clearly displayed as a direct warning to any person attempting to make a personal unsolicited approach to a place of residence to refrain from intruding onto the resident's privacy.
- (2) The surveyor ignored a pedestrian's refusal to participate in the survey. The Committee's view is that a clear verbal refusal to participate, whether at home or in a public place, should be respected.

## 2.2 Contacting Potential Informants

Contacting an informant means inviting him to participate and obtaining his consent. (Compulsory surveys are considered in 2.5.) Methods available to make contact include the mail box, telephone call, personal interview and group discussion.

### GUIDELINE (2)

*When contacting potential informants, the surveyor should:*

- (1) *recognise the possible inconvenience of approach;*
- (2) *include a frank and adequate introduction;*
- (3) *identify the interviewer;*
- (4) *avoid pressure, especially with children, the elderly and migrants;*
- (5) *include the gaining of the informant's consent before proceeding; and*
- (6) *give adequate warning of use of recording devices and observation mirrors.*

### 2.2.1 Recognise the Possible Inconvenience of Approach

The initiation of communication between the surveyor and the potential informant may be inconvenient and embarrassing on some occasions. This will be most common in telephone calls and in personal visits to the home, where the call could interrupt personal or family activities such as having a



shower or preparing or eating a meal. Public place interviews could also delay a person in a hurry. On the other hand, communications through the mail box do not entail such difficulties since the householder can choose his own time to receive the message.

The surveyor should:

- (a) avoid calling at times likely to be inconvenient to the potential informant. This will, of course, depend on the household;
- (b) recognise any inconvenience to the potential informant and offer to call back, preferably at a time nominated by the informant.

#### 2.2.2 Include a Frank and Adequate Introduction

The initial contact should include all of the following:-

- (a) in the case of telephone and personal interviews some mention of the interviewer's name;
- (b) mention of the name of the surveyor, and where it would not be prejudicial to the conduct of the survey, the name of the client also;
- (c) where appropriate, explanation of the class of informant being sought;
- (d) where a clear explanation of the survey purpose would prejudice the survey results, a general, but not inaccurate, description may be acceptable provided that it does not unduly risk the informant's goodwill. Clearly, the nature of the explanation appropriate to a particular survey heavily depends on both the sensitivity of the questions being asked and the extent to which a full explanation of purpose would prejudice the survey results (see also para. 2.3.3. Full explanation may be deferred until completion of the survey.);
- (e) where it is not readily apparent how the person came to be contacted, explanation of the source of the contact;
- (f) whether any record obtained from the interview is to be correlated with any other record about the informant obtained from any other source and, if so, what records and from what source. This is subject to comments made in 2.3.3;
- (g) invitation to participate in the survey, taking care not to imply that participation is compulsory. A more general invitation is also acceptable, e.g. "we would like your opinions". There should be a clear breakpoint before the first question is asked to enable the person to decide whether he will participate or not.

#### 2.2.3 Identify the Interviewer

In the case of personal interviews without prior arrangement, it is desirable that the interviewer should have his identification on view throughout, to enable the person to reassure himself of the interviewer's identity and affiliation. This is probably best achieved through the wearing of an identification card. Where this is not done, identification should be shown at the beginning of the interview.



In the case of telephone interviews the interviewer should state his name and affiliation at the beginning of the interview and at any time when the informant requests it.

In all cases, the person should be able to check the interviewer's authenticity by telephoning a nominated contact point. This contact point should be in the telephone directory so that the person can look it up before dialling if he so desires. The contact point should be staffed during office hours and preferably also at any time that interviewers are operating. If not, interviewers must be prepared to defer the interview until the informant has had the opportunity to check for authenticity.

In the case of unsolicited personal interviews, an introductory letter, calling card or similar, specifying the interviewer's name, affiliation and contact point should be left with the informant.

#### 2.2.4 Avoid Pressure, Especially with Children, the Elderly and Migrants

The relationship between the surveyor and the potential informant is often delicate, particularly at the early stages, and goodwill can easily degenerate very quickly into accusations of intrusiveness. It is therefore felt that it is unwise to use pressure on any informants no matter what form that pressure may take. Pressure could take the form of insistent questioning or excessive emphasis on the importance of the survey.

Special care should be taken in contacting some types of informants who may be particularly susceptible to any pressure from the surveyor. Examples would include children, particularly those under 15, the elderly and migrants.

Before children are interviewed or asked to complete a questionnaire, the permission of a parent, guardian or other person currently responsible for them should be obtained. In obtaining this permission, the surveyor should describe the nature of the interview in sufficient detail to enable the responsible person to reach an informed decision.

Similarly with the elderly and migrants, the surveyor must be satisfied that the potential informant is sufficiently informed to be able to reach his own decision as to his participation in the survey.

Surveyors who send out surveys by mail or hand delivery/pick-up should also take reasonable care in their wording of attempts to persuade those who show a reluctance, whether active or passive, to participate in the survey. Some people may believe that if they fail to respond to a survey that should be the end of the matter. A further attempt from the surveyor could therefore be both surprising and irritating. But a carefully worded re-invitation may tend to alleviate any fears of intrusion.

#### 2.2.5 Gain the Informant's Consent to Proceed

It is important that before any information is collected, the informant clearly be given the opportunity to decide whether or not he will assist. This requires that the interviewer explicitly ask for approval to proceed or invite the person's participation.



# Privacy Committee



New South Wales

---

*With Compliments*

G.P.O. Box 6, Sydney, N.S.W., 2000    Level 12, 189 Kent Street, Sydney, N.S.W., 2000  
Telephone: (02) 252 3843    Facsimile: (02) 252 3842



A general invitation is acceptable, e.g. "we would like your opinion". However, there should be a clear break-point before asking the first question.

If the survey is likely to be particularly onerous, sensitive or time-consuming then it is important that the interviewer gives the informant notice of this.

Where a particular class of person is being sought, consent should generally be gained before the questions are asked which would ascertain whether the informant does or does not qualify. However, an approach of the form: "We are doing a survey of school leavers who are having trouble finding work. Could someone help us please?" is acceptable since the person may answer by saying "no, I'm sorry", meaning either "no, there's no one here like that", or "no, I'm not prepared to help".

#### 2.2.6 Give Adequate Warning of Use of Recording Devices and Observation Mirrors

Where filming, recording or observation mirrors are part of the survey design, the informant must be given adequate warning of this (whether or not such techniques are mandatory) before he gives his consent to participate. The adequacy of the warning must be sufficient to give the informant time to properly consider his consent and must not put him in an unreasonable position of embarrassment or pressure to consent.

The Committee is available to consider questions of adequacy of warning on a case-by-case basis.

The Committee accepts that in very rare research situations there may be justification to use recording or observation techniques without first gaining the informant's informed consent. The Committee is available to consider these on a case-by-case basis. But in all such situations, the informant should be advised afterwards of such use and should be able to have all relevant records destroyed immediately on request.

#### 2.3 Collecting Information from Informants

At this stage, the informant has an adequate understanding of the survey and has consented to take part. Methods available for collection include the mail box, telephone call, personal interview, group discussion and hand delivery/pick-up. Collection may be structured in that a questionnaire is provided to the informant or at least to the interviewer. It may, however, be unstructured in which case it is a more relaxed conversation around a general topic, possibly with the aid of observation techniques and recording devices.

##### GUIDELINE (3)

*Informants should not be identified unless there is a particular need to do so. Where such a need exists, and is mandatory to the conduct of the survey, this should be communicated to the informant so that he may consider this factor in his decision as to participation.*

*There should not be any attempt to hide from the informant that he is participating in an interview in which any information collected can be interrelated.*



*There should not be any attempt to represent responses as being non-identifiable if in fact there is a way of establishing who gave the answers.*

*Care should be taken to answer an informant's questions truthfully.*

*Requests by an informant to qualify or withdraw his consent during or after the interview should be respected.*

*Any extension of the survey relationship to advertising, sales, requests for donations or other activity not contemplated by the initial contact is completely unacceptable.*

#### 2.3.1 Only Identify Informants Where There is a Particular Need

Some people do not want their answers identified but are prepared to answer questions and to have their answers recorded. This may be because of a generalised feeling that it might somehow, someday, do them harm. Accordingly, informants should not be identified unless there is a particular need to do so. The use of recording devices or observation mirrors can constitute identifiability, as can the combination of address, sex and age. See 2.4.2 below for needs foreseen by the Committee for identification of responses.

If an informant is required to be identified then the surveyor must state the purpose of the identification and agree to use it for that purpose only. The surveyor should ensure that the informant is aware of the need for him to be identified before the informant gives his consent to participate.

However, in questionnaires and straight interviews, if identification is requested but not mandatory, then it may be asked at any stage. To ensure interviewers are aware that the identification question may be declined, a refusal or non-response code should always be provided.

Frequently the informant classification questions asked may be sensitive and sufficiently detailed to effectively identify the informant. In such cases it will usually be advisable to group these questions together and provide a brief lead-in explanation of their purpose.

#### 2.3.2 Tell Informants of Any Indirect Identification

There should not be any attempt to hide from the informant the fact that he is participating in an interview in which any information collected can be interrelated. And in most situations it should be made clear to him that he is participating in such an interview and that information given in one part of the interview will be related to information given in another part. Very occasionally, as a function of the research design itself, this may not be appropriate.

There should not be any attempt to represent responses as being non-identifiable if in fact there is a way of establishing who gave the answers. The Committee has examined some methods such as hidden codes on the back or bottom of a form, the use of invisible ink, hidden cameras, hidden recording devices and undeclared observation mirrors and considers them to be subterfuges and thus improper. See 2.2.6 above for comments on consent with regard to recording and observation techniques.



In questionnaires and straight interview situations where markings are employed (which may, for instance, require the matching of two forms) the following procedures should be observed:

- (a) markings should be put in an obvious place (e.g. printed on the top right hand corner of the front page);
- (b) the survey should not be represented as being unidentified or unidentifiable. (It is perhaps true that it is unidentified but respondents may consider the surveyor is "splitting hairs" in order to hide something he is ashamed of);
- (c) the extent of the identifiability of the survey should be described as it really is (e.g. "I'm recording names of people I interview on this control sheet. At the end of the week, when the supervisor's happy I've finished all my interviews, he'll destroy this sheet and we won't have your name anywhere on our records");
- (d) on request the surveyor should explain to an informant the procedures being taken to protect confidentiality.

Non-unique marking (e.g. of geographical area) is, of course, acceptable but could cause confusion with some informants. It is therefore desirable that interviewers be able to explain the code.

#### 2.3.3 Answer an Informant's Questions Truthfully

The informant will have an expectation of the types of questions that might be asked, based on the introduction given to him. Substantially, the expectations will be based on the survey's stated purpose.

There are differing viewpoints as to how to retain the informant's goodwill, the interviewer's objectivity and the survey's success via a controlled question/answer exchange between interviewer and informant.

The Committee's feeling is that the surveyor should be aware that the sequence, logic, detail and relevance of questions may, if inconsistent with the stated aim of the survey, dissipate the informant's goodwill and arouse his suspicions. While the Committee recognises that complete avoidance of interview-created bias is impossible, awareness of the pitfalls will generally act as an incentive to avoid adverse reactions.

The Committee does, however, emphasise that care should be taken by the interviewer or surveyor to answer an informant's questions truthfully, if necessary referring to the contact point. Half-true and evasive answers are unacceptable. Where the informant asks a question, the answer to which might bias the survey, the interviewer may request postponement of any answer until completion of the interview. If the informant agrees to such postponement but is then dissatisfied with the answer to his question, the interviewer should, of course, respect the informant's prerogative to demand destruction of the record.



2.3.4 Respect an Informant's Request to Vary Consent

01  
The informant may seek to qualify or withdraw his consent during or after the interview. The request should be respected.

Three situations are envisaged:-

- V
- (a) Complete withdrawal of consent. In questionnaires and straight interview situations, if the informant asks for return or destruction of an identifiable form, this should be done, provided the request is made within seven days from the time of collection, or at any time later if the data has not yet been compiled. If compiled, particularly in identified form, it should still be deleted if it is reasonably practical to do so. Where the surveyor does not wish to release a copy of the questionnaire (e.g. for copyright reasons) he should make arrangements for destruction which are acceptable to the informant. Where mediation is needed the Privacy Committee is available to give assistance.

Where recording devices are used in an interview and the informant is the only person being interviewed, the informant's request that the recording be erased should be respected, provided the request is made within seven days from the time of recording or at any time later if the recording has not yet been analysed as part of the survey. Where other persons are simultaneously interviewed for the recording, the surveyor should exercise his reasonable discretion in considering any request by the informant to erase that recording.

Where the survey-design includes the recording of written observations about informants or correlation of interview records with any other record about the informant obtained from any other source, the surveyor should exercise his reasonable discretion in considering any request by the informant to access such observations or "other record". The Committee is available to consider questions that arise with respect to such requests, and to act as an intermediary if necessary.

- (b) Partial withdrawal of consent in respect of critical questions. Where a question exists, the answer to which is critical to the whole survey, it is reasonable to point this out to the informant. If he then insists on withdrawing, his request should be respected.
- (c) Skipping questions. This should be permitted. "Non-response" codes should be designed into the survey, particularly in the case of potentially sensitive questions.
- (d) Revising answers. This should be permitted. The answers should be recorded as the informant finally decides. There seems no reason why previous answers should not also be recorded, unless the informant specifically requests this not be done, in which case the request should be respected if practically possible. (This does not preclude re-coding by the surveyor during processing, e.g. due to inconsistent answers.)



### 2.3.5 Avoid Abuse of the Survey Relationship

Whether through a sheet of paper, a telephone call, or a personal interview, the surveyor has established a relationship with the informant, based on the stated purpose and the actual questions asked. Any extension of this relationship to advertising, sales, requests for donations, or other activity not contemplated by the initial contact is completely unacceptable. The practice of salesmen posing as interviewers is a case in point. Another example of abuse is the conduct of "market surveys" to locate individual prospects. The purpose of surveys is, in most cases, to produce statistical results, not identified responses or answers.

This is tantamount to banning the combination of surveying with almost any other activity, except possibly public relations via gift or reward. This may seem a significant constraint on commercial activity. But the Committee feels that collection of information is sufficiently sensitive in itself for the use of surveying as a source of contacts for other purposes to be undesirable.

### 2.4 Processing of Data and Publication of Results

"Processing and publication" may include:

- checking for completeness;
- tabulating to produce statistical summaries;
- correlation, or cross classification, to find out what types of informants gave what types of answers;
- play-back and analysis of interview recordings;
- follow-up, to find out the informant's answers to similar questions at a later time;
- publishing of results in quantitative or in descriptive form (and perhaps also interpretative comments);
- the quoting of individual (but not identified) responses where they illustrate an important point;
- auditing of the survey, to ensure it was suitably designed and executed;
- destroying or de-identifying the questionnaires, interview notes, recorded material and any other identified information.

The potential for privacy abuse represented by unidentifiable data is very limited. Two possible problems are:

- multi-dimensional correlation of information in the responses in order to identify the informant;
- the invasion of the privacy of a group or class of persons by the publication of statistical information.

The Committee has no evidence that these problems have ever arisen in practice, but is available for discussion on a case-by-case basis.



GUIDELINE (4)

*Identified responses should have the identification data split from other data as soon as it is practicable during the processing cycle. All identified responses should be destroyed as soon as their stated uses have expired.*

*Identification of responses should be limited to three uses: verification, play-back and follow-up.*

*Identified records should not be disseminated except to the surveyor's client or an independent auditor for verification only, or by due process of law, with due regard being given to informants' privacy.*

2.4.1 De-Identify Data as soon as Need has Expired

Previous remarks in section 2.3.1 are relevant. Responses which were required to be identified should have the identification destroyed as soon as its stated uses have expired. This may involve the destruction or de-identification of the forms (having captured the data but not the names), parts of each form, control sheets, observation notes and recorded material. Identification data should be split from other data as soon as it is practicable during the processing cycle. Audio or visual recordings should be erased as soon as their function within the survey has been fulfilled.

There is no objection by the Committee to the indefinite storage of information which has been de-identified, even if no current purpose exists and the retention is for purely speculative reasons.

2.4.2 Limit Uses of Identified Responses

The Committee foresees only three general categories of use for the identification of responses:-

- (1) for verification that the interviews in fact took place, or that the informant qualifies as a participant.

This may be required by;

- (i) the surveyor to satisfy himself as to the operation of the survey and the actions of his staff. In this case the verification can be performed shortly after collection, and the identification destroyed, precluding its use for other purposes;
- (ii) the surveyor's client or an independent auditor for the sole purpose of satisfying himself that the survey design and operation were appropriate. This may not be conveniently done so soon after collection. Nonetheless, surveyors should impose a time limit, such that requests for independent audit can only be made within some fairly short period after the completion of data collection;



- (2) for play-back where filming or recording are part of the survey design. See protections stated in 2.2.6, 2.3.4 and 2.4.1 with respect to recording and observation techniques;
- (3) for follow-up of some or all informants.

This should only be done in situations where:

- (i) the informant has been told his identity may be retained for follow-up; and
- (ii) the informant has consented to such retention.

The Committee recognises that in some situations, follow-up may be justifiable to gain consent for another interview. This may be particularly so where the original informants comprise a rare or difficult-to-trace group.

The Committee is available to consider these situations on a case-by-case basis.

Any organisation which contemplates any other use of identified/identifiable survey records should contact the Committee for consideration on a case-by-case basis.

#### 2.4.3 Restrict Dissemination of Identified Responses

The Committee has no concern at this stage with the dissemination of unidentifiable information. Dissemination of identified/identifiable records should only take place in the following circumstances:

- (a) to the surveyor's client or an independent auditor, at the request of the client, for the sole purpose of verification. The surveyor should not supply any identified responses to the client or auditor unless he is satisfied that this data will be used for the purpose of verification only. Preferably the client and auditor should be members of professional bodies which bind them to a similarly adequate set of ethics. They should inspect the material at the surveyor's premises;
- (b) to a court of law under due process with due regard being given to the sensitive relationship that exists between surveyors, informants and clients. If a surveyor considers that compliance with a subpoena would cause an unjustifiable invasion of privacy, the Committee is available to give advice on how the subpoena can be complied with and privacy protected at the same time.

If it is required to disseminate identified/identifiable records for any other purpose, the surveyor should advise the informant of all such purposes. In such instances, the surveyor should respect the informant's request not to disseminate the records.

All reasonable steps should be taken by the surveyor to ensure that the recipient of the records is aware of the importance of confidentiality and of these guidelines.



## 2.5 Compulsory Surveys: Variations to these Guidelines

The Australian Bureau of Statistics is required or authorised to collect certain statistics. Under sections 11, 14 and 16-19 of the Census and Statistics Act persons are required to answer any questions asked of them. The Committee is not aware of any other government agencies at federal, state and local level which have similar powers of compulsion to conduct surveys.

This section applies only to compulsory surveys. The full guidelines relate to all voluntary surveys irrespective of who is the surveyor or client.

Except for the Census (see Committee's background paper 32), the Committee has not studied any compulsory surveys in any depth.

In general it is felt the guidelines should apply equally to compulsory surveys, with the following exceptions and qualifications.

- (a) Re 2.1.2(a) - unidentified approach, to a home by doorknock. No protection to the householder is understood to exist in the case of compulsory surveys, although new survey topics are approved by Parliament, under s.6 (3) and (4) of the Australian Bureau of Statistics Act.
- (b) Re 2.2.2 - introductory remarks. References to voluntariness and to an invitation to participate are not relevant.
- (c) Re 2.2.5 - informant's consent to proceed. This should be qualified only to the extent that persons undertaking compulsory surveys should make every effort to obtain co-operation of informants without the need for compulsion. Communication to informants of the compulsory nature of the survey should only be made in the last resort and, if applicable and necessary to say it, with mention of penalty for non-compliance.
- (d) Re 2.3.4 - variation of consent. This should be qualified only to the extent specified in (c) above.
- (e) Re 2.4.2 - uses of identified data. Additional reasons for identification may arise. Nonetheless the responses should be de-identified as soon as such purpose has expired.
- (f) Re 2.4.2(3) - follow-up. If the law provides for follow-up, then the informant's consent need not be obtained. Even so it would be advisable to communicate this to the informant.
- (g) Re 2.4.3(a) - dissemination to an independent auditor. This will only be relevant where there is provision for audit.
- (h) Re 2.4.3(b) - dissemination to a court of law. Section 24 of the Census and Statistics Act precludes this in the case of data compulsorily acquired by the Australian Statistician. Such a provision is strongly desirable in any other legislation which authorises compulsory surveys.



3. APPENDIX I

3.1 List of Relevant Bodies

Professional Bodies

Australasian Political Studies Association  
Australian Psychological Society  
Economic Society of Australia and New Zealand  
Institute of Australian Geographers  
Market Research Society of Australia  
Public Relations Institute of Australia  
Royal Australian Planning Institute  
Sociological Association of Australia and New Zealand  
Statistical Society of Australia

Industry Bodies

Advertising Federation of Australia  
Association of Marketing Research Organisations  
Australian Association of National Advertisers  
Australian Consultant Planners Association  
Australian Direct Mail Association

Government Organisations

Australian Bureau of Statistics  
N.S.W. Statistical Co-Ordination Unit

Academic Bodies

Sample Survey Centre, The University of Sydney  
The Australian National University Survey Research Centre



APPENDIX II

4. International Code of Marketing and Social Research Practices  
Published by the International Chamber of Commerce 1977.

## Contents

	Pages
<b>Foreword</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>Basic Principles</b>	<b>7</b>
<b>Definitions</b>	<b>8</b>
<b>Rules</b>	<b>11</b>
<b>Responsibilities towards informants</b>	<b>11</b>
<b>Relations with the general public and the business community</b>	<b>14</b>
<b>The mutual responsibilities of clients and researchers</b>	<b>15</b>
<b>Reporting standards</b>	<b>20</b>
<b>Implementation of the Code</b>	<b>22</b>
<b>General information</b>	<b>24</b>
<b>ICC services to business</b>	<b>24</b>
<b>E S O.M.A.R.</b>	<b>26</b>

## Foreword

For many years the ICC and E.S.O.M.A.R. have promoted the application by all sectors concerned of rules reflecting a high level of ethics in marketing and opinion research.

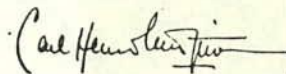
The new code of ethics set out in this publication drawn up jointly by the ICC and E.S.O.M.A.R. reflects the conviction common to both organisations that professional self-regulation can safeguard the legitimate interests of the community, while at the same time assuring the harmonious development of relations among the sectors directly involved.

The E.S.O.M.A.R. constitution requires the members of that organisation to abide by this Code.

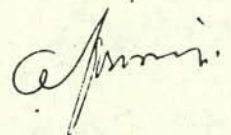
The ICC for its part recommends that all national and international professional associations representing the users and practitioners of market research adopt these rules as rapidly as possible.

Both organisations wish to emphasize that the Code includes provisions for examining any alleged failure to observe its rules of conduct.

In the near future, the ICC and E.S.O.M.A.R. plan to pursue their reciprocal efforts to foster the unification of commercial practice by issuing recommendations intended to facilitate the establishment of contracts between users and practitioners of marketing research.



Carl-Henrik Wingqvist  
Secretary General of the ICC



C.C.J. de Koning  
President, E.S.O.M.A.R.



## Introduction

---

Effective two-way communication between the suppliers and the consumers of goods and services of all kinds is vital to any modern society. Growing international links and interdependence reinforce this need. The supplier seeks to inform the consumer of what is available and where, using advertising and other forms of publicity to do so. In the other direction, the varied requirements of consumers must be made known to those who cater for their needs in both the private and public sectors of the economy, and this increasingly calls for the use of research.

Marketing research is concerned with analysing the markets for products and services of all kinds. In particular it involves the systematic study of behaviour, beliefs and opinions of both individuals and organisations. The measurement of public opinion on social, political and other issues has also long been linked with the field of marketing research; and in recent years similar approaches have been applied throughout very much wider fields of social research.

Although the subjects of study tend to differ, marketing research and social research have many interests, methods and problems in common. Both are involved with the analysis of available data, or the collection and analysis of new information, using sampling, questionnaire and other appropriate techniques. The issues dealt with in this Code therefore apply equally to both fields of research where they use similar methods of study.

It is against this background that Codes of Marketing Research Practice have been developed. The first, published in 1948 and last revised in 1972, was that of the European Society for Opinion and Marketing Research (E.S.O.M.A.R.). This was followed by a number

of Codes prepared by national marketing research organisations. In 1971 the International Chamber of Commerce (ICC), representing the international marketing community, set out to bring together and rationalise the major points contained in the existing Codes, publishing its own International Code after consultation with the marketing research and marketing bodies concerned.

Since 1971 the practice of marketing research has continued to evolve. New issues have arisen and additional safeguards have been incorporated into certain national Codes. In 1976 E.S.O.M.A.R. and the ICC both decided that it was necessary to revise their existing Codes to take account of these changes, and that it was at the same time highly desirable that there should be one international Code rather than two differing ones. A Joint Working Party representing both bodies was therefore set up to prepare a single revised Code, and this has now been adopted by the two organisations.

This international Code is designed to provide individuals and organisations concerned with a basic set of rules which are generally acceptable internationally. It applies to all international and national projects. Where in a given country there is already a national Code, the latter may on occasion go further than this international Code in dealing with certain detailed points of practice: in such cases the national Code will be followed. National and international practice must of course in all cases conform to the legislation and legal practice of the countries concerned.

## Basic principles

---

Marketing and social research depend upon public confidence: confidence that the research is conducted honestly, objectively, without unwelcome intrusion and without disadvantage to informants, and that it is based upon the willing cooperation of the public.



The general public and anyone else interested shall be entitled to complete assurance that every marketing research project is carried out strictly in accordance with this Code, and that their rights of privacy are respected. In particular, members of the general public must be assured absolutely that personal and/or confidential information supplied during the course of a marketing research study will not be made available without their agreement to any individual or organisation, whether private or official, outside the researcher's own organisation (as laid down in Section C), and that such information will not be used for any purposes other than marketing research.

Research should also be conducted according to accepted principles of fair competition, as generally understood and accepted, and to high technical standards. Marketing and social researchers should always be prepared to make available the necessary information whereby the quality of their work and the validity of their findings can be adequately assessed.

## Definitions

---

In this Code:

a) The term **marketing research** is defined as the systematic collection and objective recording, classification, analysis and presentation of data concerning the behaviour, needs, attitudes, opinions, motivations, etc. of individuals and organisations (commercial enterprises, public bodies, etc.) within the context of their economic, social, political and everyday activities. For the purposes of this Code, the term marketing research is taken to cover also social research, insofar as the latter uses similar approaches and techniques in its study of issues and problems not directly connected with the marketing of goods and services. Reference to the term marketing research shall throughout this Code therefore be held to include **social research** equally. The term also includes those forms of

research commonly referred to as **industrial marketing research** and as **desk research**, especially where these are concerned with the acquisition of original data from the field and not simply the secondary analysis of already available data.

b) The term **researcher** is defined as any individual, company, group, public or private institution, department, division, etc. which directly or indirectly conducts, or acts as a consultant in respect of, a **marketing research** project, survey, etc. or offers its services so to do. The term researcher also includes any department or division, etc. which may belong to or form part of the same organisation as that of the **client**. The term researcher is further extended to cover responsibility for the procedures followed by any subcontractor from whom the researcher commissions any work (data collection or analysis, printing, professional consultancy, etc.) forming only part of the research project; in such cases the researcher is held responsible for ensuring that any such subcontractor fully conforms to the provisions of this Code.

c) The term **client** is defined as any individual, company, group, public or private institution, department, division, etc. (including any such department or division, etc. which may belong to, or form part of, the same organisation as the **researcher**) which wholly or partly commissions, requests, authorises, or agrees to subscribe to a **marketing research** project or proposes so to do.

d) The term **informant** is defined as any individual, group or organisation from whom any information is sought by the **researcher** for the purposes of a **marketing research** project, survey, etc., regardless of the type of information sought or the method or technique used to obtain it. The term informant therefore covers not only cases where information is obtained by verbal techniques but also cases where non-verbal methods such as observation, postal surveys, mechanical, electrical or other recording equipment are used.

e) The term **interview** is defined as any form of direct or indirect contact (including observation, electro-mechanical techniques, etc.) with **informants** the result of which is the acquisition of



data or information which could be used in whole or in part for the purposes of a given **marketing research** project, survey, etc.

f) The term **record(s)** is defined as any brief, proposal, questionnaire, check list, record sheet, audio or audio-visual recording or film, tabulation or computer print-out, EDP tape or other storage medium, formula, diagram, report, etc., in whatsoever form, in respect of any given **marketing research** project, survey, etc., whether in whole or in part. It includes records prepared by the **client** as well as by the **researcher**.

## Rules

---

### A. Responsibilities towards informants

---

#### Article 1

Any statement made to secure cooperation and all assurances given to an informant, whether oral or written, shall be factually correct and honoured.

### Anonymity of informants

---

#### Article 2

Subject only to the provisions of article 3, the informant shall remain entirely anonymous. No information which could be used to identify informants, either directly or indirectly, shall be revealed other than to research personnel within the researcher's own organisation who require this knowledge for the administration and checking of interviews, data processing, etc. Such persons must explicitly agree to make no other use of such knowledge. All informants are entitled to be given full assurance on this point.

#### Article 3

The only exceptions to the above article 2 are as follows:

a) If informants have been told of the identity of the client and the general purposes for which their names would be disclosed and have then consented in writing to this disclosure.

b) Where disclosure of these names to a third party (e.g. a subcontractor) is essential for data processing or in order to conduct further interviews with the same



informants, provided that the provisions of article 4 are followed. In all such cases the researcher responsible for the original survey must ensure that any third parties so involved will themselves observe the provisions laid down in this Code.

c) Where the informant is supplying information not in his private capacity but as an officer of an organisation or firm, provided that the provisions of article 5 are followed.

#### Article 4

With the exception noted below, further interviews with the same informants shall be carried out only if:

a) Informants' permission has already been obtained at a previous interview, or

b) It is pointed out to informants at the time they are recontacted that this interview is consequent upon one they have previously given and they then give their permission before the collection of further data.

The only exception to this procedure is in the case where it is an essential feature of the research technique involved that informants do not realise that this further interview is consequent upon one they have previously given.

#### Article 5

If the informant is supplying information not in his private capacity but as an officer of an organisation or firm, then it may be desirable to list his organisation in the report. The report shall not however enable any particular piece of information to be related to any particular organisation or person except with prior permission from the relevant informant, who shall be told of the extent to which it will be communicated. This requirement does not apply in the case of secondary analysis of published data.

### Rights of the informant

#### Article 6

All reasonable precautions shall be taken to ensure that the informant, and others closely associated with him, are in no way adversely affected or embarrassed as a result of any interview. This requirement covers the information to be obtained, the interviewing process itself, and the handling and testing of any products involved in the research. The purpose of the enquiry shall be revealed in cases where information given in ignorance of this knowledge could adversely affect the informant.

#### Article 7

The informant's right to withdraw, or to refuse to cooperate at any stage of the interview, shall be respected. Whatever the form of the interview, any or all of the information given by the informant must be destroyed without delay if the informant so requests. No procedure or technique which infringes this right shall be used. Informants shall be told in advance where observation or recording techniques are to be used. This requirement does not apply where the actions or statements of individuals are observed or recorded in public places and are normally liable to be observed and/or overheard by other people present. In the latter case at least one of the following conditions shall be observed:

a) all reasonable precautions are taken to ensure that the individual's anonymity is preserved, and/or

b) the individual is told immediately after the event that his actions and/or statements have been observed or recorded or filmed, is given the opportunity to see or hear the relevant section of the record, and, if he wishes, to have it destroyed or deleted.

Wherever questions are subsequently asked to the person observed, condition (b) above shall apply.



Article 8

The name and address of the researcher shall normally be made available to informants at the time of interview. Where an accommodation address is necessary for postal surveys, or where a 'cover name' is used for interviews, arrangements shall be made so that it is possible for informants subsequently to find without difficulty the name and address of the researcher.

Interviewing children

Article 9

Special care shall be taken in interviewing children. Before they are interviewed, or asked to complete a questionnaire, the permission of a parent, guardian, or other person currently responsible for them (such as the responsible teacher) shall be obtained. In obtaining this permission, the interviewer shall describe the nature of the interview in sufficient detail to enable the responsible person to reach an informed decision. The responsible person shall also be specifically informed if it is intended to ask the children to test any products or samples.

B. Relations with the general public and the business community

Article 10

No activity shall be deliberately or inadvertently misrepresented as marketing research. Specifically, the following activities shall in no way be associated, directly or by implication, with marketing research interviewing or activities:

a) enquiries whose objectives are to obtain personal information about private indi-

viduals *per se*, whether for legal, political, private or other purposes;

b) the compilation of lists, registers or data banks for any purposes which are not marketing research;

c) industrial, commercial or any other form of espionage;

d) the acquisition of information for use by credit-rating or similar services;

e) sales or promotional approaches to the informant;

f) the collection of debts;

g) direct or indirect attempts, including the framing of questions, to influence an informant's opinions or attitudes on any issue.

Article 11

Researchers shall not misrepresent themselves as having any qualifications, experience, skills or access to facilities which they do not in fact possess.

Article 12

Unjustified criticism and disparagement of competitors shall not be permitted.

Article 13

No one shall knowingly disseminate conclusions from a given research project or service that are inconsistent with or not warranted by the data.

C. The mutual responsibilities of clients and researchers

Article 14

The relationship between a client and a researcher will generally be subject to a form of contract between them. This Code



does not aim to limit the freedom of the parties to make whatever agreement they wish between themselves. However, any such agreement shall not depart from the requirements of this Code except in the cases of certain specific articles, namely articles 15-21 inclusive, 28 and 30. These are the only articles which may be modified in this way by agreement between client and researcher.

### Property of marketing research records

#### Article 15

Marketing research proposals and quotations provided by a researcher at the request of a client and without an agreed payment remain the property of the researcher submitting them. In particular, prospective clients shall not communicate the proposals of one researcher to another researcher *except* where the latter is acting directly as a consultant to the client on the project concerned; nor shall the client use the proposals or quotations of one researcher to influence the proposals of another researcher. Similarly, the marketing research brief and specifications provided by a client remain the property of the client.

#### Article 16

The research findings and data from a marketing research project are the property of the client. Unless the prior written consent of the client has been obtained, no such findings or data shall be disclosed by the researcher to any third party.

#### Article 17

The research techniques and methods used in a marketing research project do not become the property of the client, who has no exclusive right to their use.

#### Article 18

All records prepared by the researcher other than the report shall be the property of the researcher, who shall be entitled to destroy this material two years after completion of the study without reference to the client.

#### Article 19

After the researcher has submitted his report upon the study to the agreed specification, the client shall be entitled to obtain from the researcher duplicate copies of completed questionnaires or other records, provided that the client shall bear the reasonable cost of preparing such duplicates, and that the request is made within the time limit set by article 18. Article 19 shall not apply in the case of a project or service which is developed by a researcher and where it is clearly understood that the resulting reports are to be available for general purchase on a syndicated or subscription basis. Any duplicates provided shall not reveal the identity of informants.

### Confidentiality

#### Article 20

Unless authorised to do so by the client, the researcher shall not reveal to informants, nor to any other person not directly concerned with the work of the study, the name of the client commissioning the study.

#### Article 21

All confidential information and material relating to the client shall not be divulged except to persons wholly or substantially engaged in the service of the researcher, including subcontractors, who need such information or material in order effectively to carry out the research work.



### **Client's rights to information about a project**

#### **Article 22**

The researcher shall clearly indicate to the client what parts of a project will be handled by subcontractors.

#### **Article 23**

On request the client, or his mutually acceptable representative, may attend a limited number of interviews to observe the standards of the fieldwork (he then becomes subject to Section A of this Code). The researcher is entitled to be recompensed if the client's desire to attend an interview interferes with, delays or increases the cost of the fieldwork. In the case of a multiclient study, the researcher may require that the observer in charge of checking the quality of the fieldwork is independent of any of the clients.

#### **Article 24**

When two or more projects are combined in one interview, or one project is carried out on behalf of more than one client, or a service is offered on the basis that it is also available on subscription to other potential clients, each client concerned shall be informed of this fact in advance.

### **Multiclient studies**

#### **Article 25**

The client shall not give any of the results of a multiclient study to other potential purchasers of the study unless he has first obtained the researcher's permission to do this.

### **Publishing of results**

#### **Article 26**

Reports and other records relevant to a marketing research project and provided by the researcher shall normally be for use solely by the client and his consultants or advisers. Whether or not the copyright of the research findings is reserved to the researcher in the form of contract for the project, if the client intends any wider circulation of the results of a study either in whole or in part:

a) the client shall agree in advance with the researcher the exact form and contents of publication or circulation: if agreement on this cannot be reached between client and researcher, the latter is entitled to refuse permission for his name to be quoted in connection with the study;

b) where the results of a marketing research project are given any such wider circulation the client must at the same time make available the information listed under article 31 about the published parts of the study. In default of this, the researcher himself is entitled to supply this information to anyone receiving the above-mentioned results.

c) the client shall do his utmost to avoid the possibility of misinterpretation or the quotation of the results out of their proper context.

#### **Article 27**

Researchers shall not allow their names to be used as an assurance that a particular marketing research project has been carried out in conformity with this Code unless they are fully satisfied that the project has in every respect been controlled according to the Code's requirements.



---

Article 28

In the absence of any contractual agreement to the contrary the client does not have the right to exclusive use of the researcher's services, whether in whole or in part.

---

**D. Reporting standards**

---

Article 29

The researcher shall, when presenting the results of a marketing research project (whether such presentation is oral, in writing or in any other form), make a clear distinction between the results themselves and the researcher's interpretation of the data and his recommendations.

Article 30

Normally every report of a marketing research project shall contain an explanation of the points listed under article 31, or a reference to a readily available separate document containing this explanation. The only exception to this article is in the case where it is agreed in advance between the client and the researcher that it is unnecessary to include all the listed information in the formal report or other document. Any such agreement shall in no way remove the entitlement of the client to receive any and all of the information freely upon request. Also this exception shall not apply in the case where any or all of the research report or findings are to be published or made available to recipients in addition to the original client.

Article 31

The following information shall be included in the report on a research project:

• **Background**

- a) for whom and by whom the study was conducted;
- b) the purpose of the study;
- c) names of subcontractors and consultants performing any substantial part of the work.

• **Sample**

- d) a description of the intended and actual universe covered;
- e) the size, nature and geographical distribution of the sample, both planned and achieved;
- f) details of the sampling method and of any weighting methods used;
- g) where technically relevant, a statement of response rate and a discussion of possible bias due to non-response.

• **Data collection**

- h) a description of the method by which the information was collected (that is, whether by personal interview, postal or telephone interview, group discussion, mechanical recording device, observation or some other method);
- i) adequate description of field staff, briefing and field quality control methods used;
- j) the method of recruitment used for informants and the general nature of any incentives offered to them to secure their cooperation;
- k) the time at which the fieldwork was done;
- l) in the case of 'desk research', a clear statement of the sources and their reliability.

• **Presentation of results**

- m) the relevant factual findings obtained;



U  
n) bases of percentages, clearly indicating both weighted and unweighted bases;

o) general indications of the probable statistical margins of error to be attached to the main findings, and of the levels of statistical significance of differences between key figures;

p) questionnaires and other relevant documents used (or, in the case of a shared project that portion relating to the matter reported upon).

---

## E. Implementation of the Code

---

### Article 32

Any person or organisation involved in, or associated with, a marketing research project and/or proposal is responsible for actively applying the rules of this Code in the spirit as well as the letter.

### Article 33

Any alleged infringements of the Code relating to a single country shall be reported without delay to the appropriate national body which has adopted this Code. Problems of interpretation and enforcement in such cases shall in the first place be the responsibility of the said national bodies which have adopted this Code and which are representative of all the interests directly concerned. Where such a suitable national body does not already exist it is urged that one be established speedily. The national body shall take such actions as it deems appropriate in relation to implementation of the Code, taking due account of any relevant national marketing research

Codes and the laws of the country concerned. It is important that any decision taken under this Article should be notified to the secretariats of the ICC and E.S.O.M.A.R., without revealing the names of the parties concerned.

### Article 34

In cases where:

a) an appropriate national body *does not exist*, or

b) the national body concerned is for any reason *unable* to provide an interpretation of, or take action to enforce, the Code, or

c) any of the parties involved *wishes to refer the problem to an international body* (either immediately or for a subsequent second opinion), or

d) the problem involved *parties from different countries* (for example with an international marketing research project), the problem shall be referred to the secretariats of the ICC or of E.S.O.M.A.R. The secretariats will then convene the special body set up jointly by E.S.O.M.A.R. and by the ICC for the purpose of dealing with problems of these kinds.