



PRIVACY COMMITTEE

GOODSELL BUILDING
8-12 CHIFLEY SQUARE, SYDNEY
BOX 6 G.P.O., SYDNEY, N.S.W. 2001
TELEPHONE: 238 7113
REF. MJF

BP 48

November 1978

THE COLLECTION, STORAGE AND DISSEMINATION
OF CRIMINAL RECORDS BY THE POLICE

This is the third in a series of papers on Criminal Records conducted by the New South Wales Privacy Committee.

The first report which examines the Use of Criminal Records in the Public Sector, will be released before the end of this year. A background paper to this report (BP41) was made available in November 1977.

The second report concerning the Special Branch - Criminal Records in N.S.W. (BP45) was released in March 1978.

This background paper is published for public discussion, comment and criticism. No firm decisions on its contents or proposals have yet been taken by the Committee.

Further reports on Criminal Records are planned and particulars of the whole study programme in this area can be found in Criminal Records and their Uses in N.S.W. (BP19 September 1976).

Submissions should be forwarded to the Committee at the above address by 28 February 1979.

53992

COLLECTION, STORAGE AND DISSEMINATION OF CRIMINAL RECORDS
BY THE POLICE DEPARTMENT

| <u>Para.</u> | | <u>Page</u> |
|--------------|--|-------------|
| | <u>CHAPTER ONE: INTRODUCTION</u> | |
| 1.1 | Introduction | 1 |
| 1.2 | The Committee's Study on Criminal Records | 1 |
| 1.3 | What the Criminal Records Office Contains | 1 |
| 1.3.3 | Other Stores of Criminal Record Data in N.S.W. | 2 |
| 1.4 | Why is a Store of Criminal Records Necessary? | 2 |
| 1.5 | Storage and Dissemination of Criminal Records and the Protection of the Subject's Privacy | 3 |
| 1.6 | Completeness and Accuracy of Files as Privacy Safeguards | 4 |
| 1.7 | Records and Rehabilitation of the Offender | 5 |
| | <u>CHAPTER TWO: DESCRIPTION OF THE CRIMINAL RECORDS OFFICE</u> | |
| 2.1 | Collection of Data | 6 |
| 2.1.3 | Photographs | 6 |
| 2.2 | The Criminal Records Office - Diagram and Structure | 7 |
| 2.3 | Central Card Index | 6 |
| 2.3.1 | Record Cards | 6 |
| 2.4 | Central Fingerprint Bureau | 8 |
| 2.5 | Photographs | 8 |
| 2.6 | Civil Index | 8 |
| 2.7 | Juvenile Records Index | 8 |
| 2.8 | Shoplifters' Index | 8 |
| 2.9 | Modus Operandi | 8 |
| | <u>CHAPTER THREE: DATA COLLECTION, FINGERPRINTS AND PHOTOGRAPHS</u> | |
| 3.1 | Fingerprints and Photographs for Identification | 10 |
| 3.2 | The Committee's View on Fingerprints | 10 |
| 3.3 | Obtaining Fingerprints | 11 |
| 3.3.2 | When Police can Fingerprint | 11 |
| 3.3.7 | The Discretion to Fingerprint | 13 |
| 3.4 | Photographs | 14 |

| <u>Para.</u> | | <u>Page</u> |
|--------------|---|-------------|
| | <u>CHAPTER FOUR: DATA SECURITY, PHYSICAL SECURITY AND ACCESS TO DATA</u> | |
| 4.3 | Data Security - Physical | 16 |
| 4.4 | Accesses | 16 |
| 4.5 | Logging of Accesses | 17 |
| 4.6 | Frequency of Access | 17 |
| 4.7 | Unauthorised Access | 17 |
| 4.7.5 | Possible Reform to the Present Security Check System | 19 |
| 4.8 | Voluntary Disclosure by Police | 21 |
| 4.8.4 | Proposed Amendments for Police Rules - Proposal 6 | 22 |
| 4.9 | Individual Access | 22 |
| | <u>CHAPTER FIVE: RETENTION</u> | |
| 5.1.1 | Destruction or Archiving | 26 |
| 5.1.2 | Need for Retention of Police Records | 26 |
| 5.2 | Unsuccessful Charges | 26 |
| 5.2.2 | Fingerprints and Photographs | 27 |
| 5.2.3 | Court Appearances and Arrest Details | 27 |
| 5.2.4 | Intelligence Requirements | 28 |
| 5.2.5 | Destruction on Request | 28 |
| 5.3 | Section 579 Crimes Act | 30 |
| 5.4 | The Culling Programme | 33 |
| 5.5 | Destruction/Archiving | 35 |
| 5.6 | Recordable - Non-recordable Criminal Record Information | 35 |
| 5.7 | Decriminalised Offences - Deletion or Retention? | 36 |
| 5.8 | Culling or Deletion on Access | 37 |
| | <u>CHAPTER SEVEN: COMPUTERISATION</u> | |
| 7.1 | Computerised Records | 39 |
| 7.2 | Police Records Presently Stored on Computer | 39 |
| 7.3 | Specific Proposals for Conversion of Other Police Data Systems to Computer Storage | 40 |
| 7.4 | Access to Computer Storage | 41 |
| 7.5 | Linkages | 41 |
| 7.6 | Privacy Concerns in the Computerisation of Criminal Record Data | 42 |

| <u>Para.</u> | | <u>Page</u> |
|--------------|---|-------------|
| 7.6.3 | Centralisation and Growth of Records | 42 |
| | <u>CHAPTER EIGHT: JUVENILE SHOPLIFTERS' INDEX</u> | |
| 8.1 | History | 44 |
| 8.2 | Present Procedures | 44 |
| 8.3 | Problems with the Shoplifters' Index | 46 |

COLLECTION, STORAGE AND DISSEMINATION OF CRIMINAL RECORDS
BY THE POLICE DEPARTMENT

| | | <u>Page</u> |
|----------|--|-------------|
| Proposal | 1 Fingerprinting | 12 |
| | 2 Expansion of Logging | 19 |
| | 3 Random-Ring Back System | 20 |
| | 4 Verification of Random Checks with Data Subject | 20 |
| | 5 Penalties for Illegal Access | 21 |
| | 6 Amendment of Police Rules on Disclosure | 22 |
| | 7 Penalties for Unauthorised Disclosure | 22 |
| | 8 Photocopies of Court Appearances | 25 |
| | 9 Automatic Destruction on Dismissal | 30 |
| | 10 Amendment to s579 | 33 |
| | 11 Culling and Destruction | 34 |
| | 12 Destruction of Records | 35 |
| | 13 Retaining Records of Repealed Offences | 37 |
| | 14 Juvenile Shoplifters' Index: Access by Nominated Firms | 44 |
| | 15 Exchange of Information | 45 |
| | 16 Police Employment Purposes | 45 |
| | 17 Separate Maintenance of the Index | 45 |
| | 18 Destruction of Duplicate Forms | 45 |
| | 19 Destruction of Cards | 45 |
| | 20 Parental Signature on Report Form | 46 |

COLLECTION, STORAGE AND DISSEMINATION OF
CRIMINAL RECORDS BY THE POLICE DEPARTMENT

1.1 CHAPTER 1: INTRODUCTION

1.1.1 The Need to Study Criminal Records

"Information about crime and suspected crime noted in Police, Court, and Prison records comprises one of the most extensive personal record systems kept by the public sector in this State. It contains some of the most potentially prejudicial information of any information." (1)

The largest repository of crime data in N.S.W. is the Police Department's Criminal Records Office (to be referred to as CRO). Therefore, to adequately consider any privacy issues raised by the maintenance of criminal records, the Committee examined the major point of storage and dissemination of such records.

1.2. The Committee's Study on Criminal Records

1.2.1 The collection and storage of criminal information by the Police Department in the form of the CRO, provides the basic reference for the various users of criminal records in N.S.W. (for both Police, Public Authority and Court use).

The Committee has recently completed two aspects of its overall examination of the privacy aspects involved in the use of criminal records:

- (i) the Fair Use of Criminal Records in the Public Sector;
- (ii) the intelligence information stored by the N.S.W. Special Branch.

Following the release of this current report, the Committee intends to examine criminal records as they specifically relate to juvenile offenders.

The discussion of areas more directly relevant to these other aspects of the Committee's overall criminal records study will be limited in this report to where they specifically influence CRO procedures.

1.2.2 Following a general outline of the functions of the CRO, this report will concern itself with particular CRO practices relating to the collection, storage, retention, access and security of criminal record information. Chapters 3 to 8 develop the Committee's Draft Policies as they relate to the aforementioned practices.

1.3 What the Criminal Records Office Contains

1.3.1 The CRO obtains details of criminal charges, dismissals, convictions, sentences and appeals from both internal Police documentation and Court records. The principal source of fingerprint and photograph records is at the stage of laying the charge (pursuant to Crimes Act s353A.) (2) Personal details of the subject such as name, address, age, physical characteristics, etc. are also obtained by the charging officer. Information as to the granting or refusal of bail, dates of court appearances, the court's determination, the sentence imposed and details of appeal,

(1) Privacy Committee, First Annual Report (March 1976) page 21

(2) At present, the Police have no power to have a person remanded back into their custody after conviction for the purpose of fingerprinting, except under the provisions of s558, Crimes Act

may be obtained from the relevant court papers. Matters relating to the breaching of a recognizance or the forfeiture of bail would also be noted on these papers.

1.3.2 CRO as Interstate Record Store

The CRO is the only complete and permanent record of criminal information in the State. Its records include virtually all charges and subsequent court appearances by both adults and juveniles, indexed by the offender's name, aliases and fingerprints. It does not include the relatively small number of offenders, whom the Police choose not to fingerprint.

The wider function of the CRO is that of the Central Criminal Record index for all Australian police forces. Although the CRO is run by officers of the N.S.W. Police Force and State public servants, all costs of the operation of the CRO are shared among all police forces in Australia on an agreed formula. The principles under which the CRO maintains other states' and Commonwealth data are determined by conferences of police commissioners.

Criminal record information accumulated by state police forces is (in principle) conveyed to the CRO for central storage and access. Thus the CRO acts as the Australian "clearing house" for criminal records.

1.3.3 Other Stores of Criminal Record Data in N.S.W.

Although criminal record information is held by certain State Government Departments, none possesses data as wide ranging as the CRO's. The Department of Youth and Community Services maintains a system of records related to juvenile offenders and the Department of Motor Transport keeps data on offences relating to motor vehicle and public vehicle licences. Each court maintains records of the offenders who appear before it, however, there is no central index of all court records. The Department of Corrective Services has a comprehensive system of data specifically related to offenders sentenced to terms of imprisonment. There are many other smaller stores of criminal information for specific purposes (e.g. employment, registration, etc. - See BP 41).

1.4 Why is a Store of Criminal Records Necessary?

1.4.1 A central record of criminal data is presently required in the following situations:-

- (i) where disabilities are created by statute, restricting or prohibiting the actions of an individual with a criminal record;
- (ii) where a past criminal offence is disclosed in response to a question on certain application forms (also if pending charges are disclosed, in some cases) and a CRO check is requested;
- (iii) where CRO checks are specifically requested in relation to applications for employment, licensing or holding certain benefits;
- (iv) where regular CRO checks are carried out on the renewal of certain licences or benefits; (3)
- (v) checks for general police purposes.

(3) When a person appears before a court and is an employee, licensee or benefit holder of certain public departments or authorities (see BP41) the Clerk of Petty Sessions is required to report that court appearance to any such public body.

1.4.2 Therefore, it might be assumed that the three major types of access that would be made to information held at the CRO are:-

- (i) Police administration and investigation procedures;
- (ii) judicial and magisterial administration and sentencing where the Court may require assistance in deciding on applications for bail or sentencing. Here criminal record information will be presented by the Police.
- (iii) non-Police uses, e.g. employment checks, licensing investigations, decisions on the granting of administrative benefits, etc. (4)

1.4.3 The Committee has expressed its interest in criminal history information in its paper on the Use of Criminal Records in the Public Sector (BP41). However, its interest in such information extends beyond the question of public sector use to police use. Regardless of the type of use to which its records are put, the CRO might pose a positive danger to the privacy of the individual if the information it holds was inaccurately maintained or improperly accessed. By raising these problems, the Committee does not wish to suggest that the present practices of the CRO are generally incorrect or deficient; quite the reverse. The Committee has been very favourably impressed with the administration of the CRO, both in its measures for accuracy and security. As this report will recommend, the major proportion of CRO practices should continue unchanged.

1.5 Storage & Dissemination of Criminal Records and the Protection of the Subject's Privacy

1.5.1 One objective of this report is to describe the criminal record storage and dissemination practices of the Police Force so that the current control and the regard for the security of this type of data is apparent. Many complaints received by the Committee in this area evidence a general ignorance about such records throughout the community which, in turn, often fosters unjustified fears. The overriding desire of the CRO for complete, accurate and reliable records corresponds with their concern that their records remain secure and available only to those with authority to access the data. In the proposals set out in this report it has been the Committee's intention to enhance the protection of the privacy of the individual without unduly restricting the effective and necessary functions of the system.

1.5.2 It has been argued that because the original occurrences on which this data is based, e.g. police investigations and court hearings, may be public in nature, the records should be available for general access. However, the many and varied ways in which this information is used may not be contemplated by the court as an element of its sentence or a direct result of the conviction. It would be fair to assume that neither the convicted party nor the court fully realises the extent of the access and the variety of uses for criminal record information. Privacy concerns may not be raised by the criminal record itself, yet such issues must be considered when the information is stored and disseminated for a variety of third party purposes, i.e. non-Police or court use. However when an extensive record system such as that maintained by the CRO has the potential to affect the privacy of the individual subject, a dual responsibility rests with both the record keeper and those using the records, to be ever mindful

(4) (For information as to the public sector bodies who receive criminal record information from the CRO and under what circumstances such information is given, consult the Committee report on Public Sector Uses of Criminal Records.) BP 41, November 1977.

of this potential and to guard against any action which will be an unjustified invasion of the subject's privacy.

1.6 Completeness and Accuracy of Files as Privacy Safeguards

1.6.1 It is generally accepted that privacy concerns are magnified by the storage and dissemination of inaccurate or incomplete information. The threat to the privacy of a file subject posed by the storage of criminal record data is directly influenced by the way in which such information is disseminated.

As was stated in Farlton -v- Saxble (5):-

"Dissemination of inaccurate criminal information without the precaution of reasonable efforts to forestall inaccuracy, restricts the subject's liberty without any procedural safeguards designed to prevent such inaccuracies."

It has been suggested that the following procedures should be the aspiration of any storer of criminal record data to ensure the accuracy and completeness of such information.

- "(1) Every item of information should be checked for accuracy and completeness before its entry into the system.
- (2) A system of verification and audit should be instituted. Files must be designated to exclude ambiguous and incomplete data elements...Where files are found to be incomplete, all persons who have received misleading information shall be immediately notified." (6)

1.6.2 The CRO ensures the accuracy of its data in two ways:-

- (a) it does not record any entries on a subject if such entries cannot be verified by fingerprints; (7)
- (b) it provides at the request of the subject a copy of the relevant criminal information data so the accuracy and completeness of such data can be ascertained to the satisfaction of the subject.

The CRO also presumes that the information it receives from the Clerk of the Court as to the Court's disposition of a particular charge will be accurate. It does concede, however, that the delay in receiving notification of data from certain interstate sources, be they the Police or the Courts, and the failure to be notified of the disposition of certain appeals may lead to some records being incomplete.

1.6.3 The Committee has endorsed the use of fingerprints as a method to verify the subject of a record. It is also satisfied with the present procedure for subject access as another check on the accuracy of the information. With the implementation of the Committee's proposal for the destruction of data relating to unsuccessful charges (para. 5.2.8) the proposals concerning the Shoplifters' Index (para. 8.3.2) and its general proposals on data security and disclosure by Police (ch. 4), it is hoped that both the accuracy and completeness of the record system and the ensuing dissemination of that data will be enhanced.

-
- (5) 507 F.2d 1116 (D.C. Cir. 1974)
 - (6) Madden J. T. & Lessin M. S., Privacy: A Case for Accurate & Complete Criminal History Records. 22 Villanova L.R. 1171 at 1198
 - (7) It does not, however, delete entries when a person successfully applies to have his fingerprint records destroyed.

1.7 Records and Rehabilitation of the Offender

When the Committee's proposals concerning the culling and destruction of old records (para. 5.4.3) are viewed in conjunction with its guidelines for the fair use of criminal record data (see BP 41), most individuals who have not re-offended for the ten year period should not be adversely affected by the original offence. This approach to the rehabilitation issue has considered the conflicting interests of both the offender, who should have the chance to live down first mistakes and the Police who require complete records to fulfil their normal investigative function. Criminal record information is, however, widely accessed by Public Authority and court users in this State and therefore some compromise in the record system is necessary to protect the interests of the "rehabilitated" offender.

CHAPTER 2: DESCRIPTION OF THE CRIMINAL RECORDS OFFICE

2.1 Collection of Data

2.1.1 Fingerprints

The CRO only records details of offences if they are supported by fingerprints.

2.1.2 Fingerprint information at the CRO is held on a fingerprint form in the central fingerprinting bureau (Appendix 1). This form is completed when the person is charged. This is the major source of CRO identification data and is one of the two main sources of information for the CRO record cards. The other is the result of present charges forms (Appendix 2).

2.1.3 Photographs

Existing Police policy is that everyone who is fingerprinted should be photographed. In practice, however, only about 15,000 offenders are photographed annually (approximately 25% of those fingerprinted).

2.2 The Criminal Records Office

On the following page is a diagram of the structure of the Criminal Records Office.

2.3 Central Card Index (CCI)

The Central Card Index is the record of all information stored where fingerprints are received and the results of charges.

2.3.1. Record Cards

The record cards are of standard form (Appendix 3). The following information is recorded on such cards:

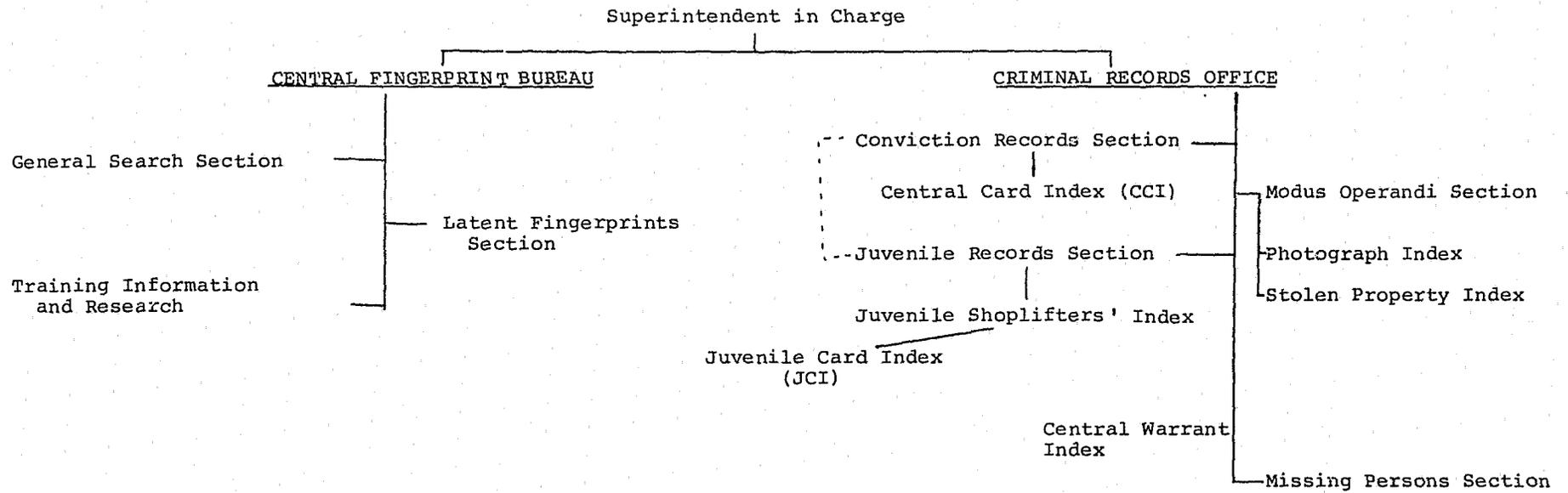
- (a) full name, date of birth, fingerprint classification, description, photo, reference. The date recorded is that taken when the person is fingerprinted. Where the subject's identity is not established by fingerprints, offences are not recorded;
- (b) all convictions, sentences, findings, dismissals and appeals are recorded in the terminology of the Court before which the person appeared, e.g. see reverse side of card (Appendix 3);
- (c) the date and court of hearing are recorded, the issue of any warrant and "wanted" entries. A cross reference is made to any person with whom the subject might have been arrested.

2.3.2 There are approximately two million names recorded at the CRO. Additions are currently made at the rate of approximately 50,000 names per annum. Deletions consist primarily of deceased persons and such deletions are transferred to microfilm. There are approximately one thousand (1,000) per annum.

2.3.3 If a juvenile is fingerprinted, a fingerprint form and a record card will be maintained on him at the CRO. This card will contain the same particulars as the card held by the Juvenile Records Section (JRS). If the juvenile is not fingerprinted, he will not have a CRO card, only a card at the JRS. Whilst the JRS card will be culled soon after his eighteenth birthday, the CRO card will not.



DIAGRAM OF ELEMENTS COMPRISING C.R.O. & C.F.B



2.4 Central Fingerprint Bureau

The fingerprint and identification information appearing on forms P59 or P59(a) (Appendix 1) are stored separately on visual strip indexes (Appendix 4). Copies may be kept available for sending to either Police stations or interstate and overseas Police Departments.

2.5 Photographs

- 2.5.1 At the time that photographs are taken, an identification card (Appendix 5) is filled out and one fingerprint is marked on the card, to overcome the problem of incorrect names being given. This acts as a double check that fingerprints, photographs and charge details have been received and correspond.
- 2.5.2 Multiple copies of the photograph may be produced, depending on the nature of the crime and transferred to another Units, e.g. Criminal Intelligence Unit or Modus Operandi. Extra copies of the photographs may also go on category files in Modus Operandi, e.g. drugs, shoplifters, car stealers, etc.

2.6 Civil Index

- 2.6.1 A Civil Index is kept as a Civil Bureau containing the fingerprints supplied for visa purposes. This is used when a foreign embassy inquires about the possible criminal record of any applicant for a visa. Primarily such inquiries are made where the stay is an extended one rather than for normal tourist purposes. No reference is made to this file for other than visa applications. The file is automatically destroyed at the expiration of each ten year period.

2.7 Juvenile Records Office (Juvenile Record Index)

- 2.7.1 This index comprises cards (Appendix 6) kept in alphabetical order. There is no strict index nor are there any references to fingerprints. If the juvenile was fingerprinted then that record would be duplicated in the central card index and the fingerprints kept in the central fingerprint bureau.
- 2.7.2 The juvenile records are microfilmed every five years when the young person attains the age of 20 years. This record is regarded as dormant and can only be referred to in most unusual circumstances, e.g. if the person was murdered or reported missing.

2.8 Shoplifters' Index (See Chapter 8)

2.9 Modus Operandi

- 2.9.1 The Modus Operandi section contains the following information:
- (a) the central index of all photographs alphabetically listed and in subject categories. Local police stations order copies of photographs taken locally which they consider to be necessary for local purposes. Both the M.O. and local photograph books are used for witness perusal;
 - (b) information included in Crime Incident Reports. This data is sent to the M.O. by officers who have received details of the occurrence of certain crimes. As further information is gathered concerning these incidents it will be fed into the M.O. to build up a complete picture of the offence. If a charge is eventually made and a determination given by the Court, this will be referred to the M.O. from CRO files.

- (c) "Consorting" files - When individuals are seen in the company of known criminals this may be noted by the Police and recorded on consorting cards at the M.O.
- (d) Stolen Property Index - details of stolen property (e.g. description, serial numbers, etc.) are recorded at the M.O. These are regularly compared with the records of pawn brokers and other money lenders in an effort to trace stolen goods.

2.9.2 For a discussion on the use of photographs by M.O. see para. 3.4.3 et seq.

2.10 Computerisation

As the Police Department is presently involved in an extensive feasibility study of the most effective introduction of computerised records, a full discussion is included in chapter 9.

2.11 Microfilming

A microfilm filing system is maintained of cards culled from the various card indexes and kept in separate but related storage. The developing of the exposed film is currently done by Kodak (Australasia) Pty. Ltd.

CHAPTER 3: DATA COLLECTION - FINGERPRINTS AND PHOTOGRAPHS

3.1 Fingerprints and Photographs for Identification.

To accurately associate data collection with its subject, it is necessary to also accumulate positive identifying information. The Police have relied primarily for this purpose on fingerprints and, to a lesser extent, photographs. The CRO will only record details of offences if they are supported by fingerprints.

3.1.2 Police in N.S.W. fingerprint every person who is arrested, for any offence, with the exception of 17 minor offences specified in Police circular 74/109.

3.1.3 Fingerprinting is usually only possible where the person is arrested and therefore a CRO record may not be opened or noted in situations where the arrest does not take place. This means that information laid by a private citizen, and many statutory offences prosecuted on summons by the Police or a government department, will not be noted at the CRO. (See para. 3.3.7.)

S352 of the Crimes Act allows the Police to arrest for any offence under any Act. This power is obviously not used in the case of many statutory offences. It seems that the N.S.W. Police almost invariably proceed by arrest for any offence against the Crimes Act, Summary Offences Act, etc. Arrests under warrant for non-payment of fines or failing to obey the order of the Court, will also be noted at the CRO.

3.1.4 The Police consider it necessary to identify persons to the Courts and to make known the fact that that person has or has not previously failed to appear when released on bail, that he is a former prisoner subject to licence or parole, or that he is at large by virtue of entering a recognizance with certain conditions. At present it must surely be of importance for Courts to be aware of the fact that an accused person is undergoing periodic detention or is involved in a work release programme.

Aliases are widely used by persons in custody and, if correct identity is not established, offenders wanted as escapees, on warrant or for questioning regarding other offences could pass through Police hands without being detected.

There is also the possibility that the person charged could subsequently disappear or escape and particulars of his identity be needed.

3.2 The Committee's View on Fingerprints

3.2.1 The Committee generally opposes the use of fingerprints as an identification method because of the degree of physical intrusion involved. But criminal records are so potentially damaging that to ensure maximum accuracy, fingerprinting is essential.

3.2.2 Fingerprinting provides two major safeguards:-

- (a) it minimises the possibility of mixing two persons' records under the one subject's name;
- (b) it allows a person to prove a record is not his even though recorded under his name, address and date of birth.

3.2.3 For these reasons the Committee opposed the proposals to reduce fingerprinting contained in the Criminal Investigation Bill 1977(Commonwealth). (1)

3.3 Fingerprints

3.3.1 Obtaining Fingerprints. Two questions arise when one considers the Police fingerprint power, conferred by s353A of the Crimes Act, 1901. (2) They are:

(i) when can the Police require an individual to submit to fingerprinting?

(ii) to what degree may force be used to effect the process of fingerprinting?

3.3.2 When Police can Fingerprint. A recent advice from the Crown Solicitor suggests that this only means "where necessary to obtain evidence of the crime" i.e. not simply so that an accurate CRO check can be done for bail or sentencing purposes. This section applies when a person has been charged with an offence and only while such a person is in lawful custody; during the period between the laying of the charge and the admission of the accused to bail, or if he is not admitted to bail, until he is brought to trial. The power is discretionary on the officer in charge of the station where the accused is in custody, but goes no further. It does not impose any obligation on the accused to furnish particulars or to submit to having his fingerprints taken.

3.3.3 The Crimes Act s558(3) dealing with first offenders empowers the Police to remove the offender to a gaol or other place determined by the court and there "submitted to the examination customary for securing further identification".

"s558(3) When such recognizance is entered into the offender may be removed to such a gaol, or other place, as the court may determine, and there forthwith submitted to the examination customary for securing future identification. Detention for this purpose shall not exceed a term of forty-eight hours and the offender shall thereupon be discharged from custody."

This section only relates to where a recognizance is imposed by the court and is rarely used.

3.3.4 Use of Force. The Court of Criminal Appeal in R v Carr (1972) 1 N.S.W. LR 608, stated that the common law gave the Police the power to take prints for identification to the court and that s353A "merely gave a statutory recognition to taking fingerprints by force in certain circumstances." There is, however, doubt whether the Police have power to take fingerprints for record purposes.

(1) Submission on the Criminal Investigation Bill 1977 (Cwth). Privacy Committee BP 33 May 1977.

(2) S353A "Where a person is in lawful custody for any offence in charge of the police station where he (sic) is so in custody may take or cause to be taken all such particulars as may be deemed necessary for the identification of such person, including his photograph and fingerprints and palm prints."

If, as stated above, it is essential for accuracy of the records to fingerprint then it would be desirable to amend section 353A to provide clear power for the use of reasonable force in taking fingerprints. (3)

- 3.3.5 The Commissioner of Police has recommended to the Premier that s353A(c) be amended by the deletion of the present subsection and the insertion of the following in its place:

"every person in lawful custody shall be liable to be photographed and to have his fingerprints and palm prints taken. The officer in charge of police at the station where he (sic) is in custody may take or cause to be taken such photograph, fingerprint and palm prints of such person, using no more than necessary."

- 3.3.6 Excluded from the recommendation in para. 3.3.5 are the increasing number of proceedings initiated by summons rather than arrest and charge. Discussions with Police and Corporate Affairs Officers have revealed that fingerprints are primarily required from persons committed for trial rather than those dealt with summarily on summons. Where a person is dealt with by a summons no fingerprints are taken. Summonses are less privacy intrusive than arrest and charge and are therefore to be encouraged whenever appropriate.

3.3.7 Proposal (1)

Every person

- (a) *who is in lawful custody on being charged;*
- (b) *on being committed for trial for any offence*

-
- (3) An alternative is the detention of any party refusing to be fingerprinted, pending a hearing before a magistrate as to justification. This would require the magistrate to hear submissions from both the Police and the individual refusing to be fingerprinted. The onus of proof as to the necessity for such an order should rest with the Police. Following the granting of such an order, if the person continues to refuse, detention on the basis of contempt for the order may be justified. The use of any physical constraint to prohibit a person's freedom of movement or self-determination, should be seen as an ultimate privacy invasion.

Such a process would be drawn out and might involve far greater interference with the privacy of the individual than any suggestion of the use of reasonable force. The necessity for fingerprinting, as recommended by the Committee, is clearly established and the facts of custody and charge appear to be an adequate threshold. If an occurrence is sufficiently serious to warrant custody and charge, or committal for trial, then that seriousness justifies fingerprinting.

The suggestion that in certain situations fingerprinting should be done on conviction, would necessitate the creation of a power to allow the Police to have an individual remanded back into their custody for the purpose of fingerprinting. The only similar power is conferred to a limited degree by s558. Any extension of the power should be avoided.

shall be liable to have his fingerprints and palm prints taken and to be photographed. The officer in charge of the Police station where the person is in custody may take or cause to be taken such fingerprints, palm prints and photographs of such person using no more force than is reasonable under the circumstances. (The Act should also be amended to provide that the magistrate shall make an order remanding a person into lawful custody for the purposes of having his fingerprints taken on being committed for trial on any offence at the request of an officer of the N.S.W. Police Department.)

A person may also consent to have his fingerprints or photographs taken. However, as such consent may be withdrawn at any time until they are taken, consent has not been included in this proposal.

3.3.8 The Discretion to Fingerprint

At present the provisions in the Crimes Act relating to fingerprinting are discretionary. The Committee agrees that this should be retained.

Police are instructed on the circumstances under which a person in lawful custody is or is not to be fingerprinted by Police instruction number 25, paragraph 18, qualified by paragraph 11 and Police Circular No. 74/190.

Police Instruction No. 25.

- (a) Paragraph 18: "Where a person is in lawful custody for any offence punishable on indictment or summary conviction, the officer in charge of Police at the Station where he is in custody may take, or cause to be taken, all such particulars as may be deemed necessary for the identification of such person, including his photograph and fingerprints.

This power is conferred by S353A(3) of the Crimes Act, 1900, but should, however, be exercised with discretion and the instruction given in paragraph 11 respecting minor offences should not be overlooked."

- (b) Paragraph 11: "When a person is in lawful custody on a charge (except in cases of drunkenness, drunk and disorderly, carrying away liquor during prohibited hours or being on licensed premises), notwithstanding that his criminal record has been previously furnished by the Criminal Records Office the fingerprints of the offender should be taken in every instance at the earliest opportunity subsequent to his being charged, and forwarded direct to the Criminal Records Office without delay. Where a suspicious stranger is charged in a country district of even a minor offence and it is considered desirable to trace his antecedents, his fingerprints should be taken and transmitted to the Criminal Records Office immediately. Police at the Station where the offender is charged will be responsible for seeing that these instructions are strictly complied with."

- (c) Circular 74/190

"Police generally are advised that fingerprints are NOT now required to be taken for the following charges:

- * drunkenness
- * drunk and disorderly
- * carry away liquor during prohibited hours
- * being on licensed premises
- * refusing to quit licensed premises
- * consume liquor in park
- * disobey order of maintenance
- * set up stand
- * commitment warrants
- * riotous, indecent, threatening, insulting manner
- * unseemly words
- * gaming or betting offences other than manager or principal
- * trespass on railway
- * drunk on railway
- * evade fare
- * breaches of Regulations under the Traffic Act, where the driver is licensed and has adequate proof of identity

So far as fingerprinting in "offensive manner" cases are concerned, the taking of fingerprints in those cases is to be at the discretion of the member accepting the charge. The member in arriving at his decision would require to take into account the seriousness of the circumstances as related to him by the arresting Police, and whether or not the person charged is known or suspected to be an old offender, whose lapse it would be advisable to have on record."

- 3.3.9 Circular 74/190 increased the list of offences for which fingerprints were not required and therefore not recorded in CRO. This may have been due to the difficulty of processing the ever increasing number of fingerprints taken rather than any other reason. It is, however, de facto recognition that not all offences are "criminal" in its broad sense.

3.4 Photographs

- 3.4.1 Many of the issues raised in respect of fingerprints apply equally to the collection of photographs. S353A of the Crimes Act provides for photographs to be taken in the same way as fingerprints. The comments on the limitations of s353A and fingerprinting are also applicable to the power to photograph. The Police proposals for amendment would empower them to photograph anyone in custody.

3.4.2 Current Photographing Practices

Although this is not the case in practice, Police policy is that everyone who is fingerprinted should be photographed. Photographs of offenders are taken at numerous Police Stations throughout the State. Completed films are sent with a form and card to the Scientific Branch of the CIB for processing. Having been checked for accuracy, the card is forwarded to the CRO for notification on the offender's CCI card and the photograph is forwarded to the Modus Operandi Section.

On receipt of the photograph, particulars are noted and the photo is catalogued by date of birth. When the photograph identification card is received by M.O. from the CRO, details are again checked and other copies of the photograph are obtained (e.g. height, distinguishing features, sex, type of offence, deformities, etc.). Further copies may be sent to local Police Stations on request. Cards are filed numerically for retrieval if further copies are necessary. Negatives are retained in the MO photo room for up to 9 years (approximately 700,000 photos).

3.4.3 Viewing Photographs of Suspects

Witnesses attend the MO section where they are interviewed to obtain details of the crime and a description of the offender. From this information the appropriate category is selected for the witness to view. In the past 3 years less than 5% of witnesses inspecting the books have made positive identifications and approximately one tenth of those positive identifications have turned out to be incorrect.

3.4.4 Extension of the Use of Photographing

Every year 15,000 persons, or approximately 25% of those fingerprinted are photographed. Extensive use of photographing cannot be justified on the same grounds as the fingerprinting practices. Photographs are not necessary to maintain the accuracy of the CRO. Their use may be an aid to crime detection. However this is limited by the currency of the photograph. The principal benefit in the retention of photographs is to assist witnesses in identifying offenders and generally stimulate the collection of evidence concerning an offender. However maintaining photographs is a far more obvious intrusion into the individual's privacy than maintaining fingerprints. The inclusion of a person's photograph in a police photo book, basically retained for perusal by members of the public who have witnessed a crime, creates the problem of labelling.

The appearance of the photograph of an acquaintance in such books may imply to a witness perusing these records, that the acquaintance is a criminal.

3.4.5 Both the Committee and the Police agree that there are certain problems peculiar to the current photographing process.

The Police state that the disadvantages connected with the current system of handling viewing, storing and distributing photos are as follows:

- (a) extensive delays exist between the photographing of an offender and the time the photo is available for viewing at the MO section;
- (b) due to the lack of trained photographers at local Police stations many of the photos are of poor quality. Duplication at station level may also occur;
- (c) excessive copies of photos produced;
- (d) poor physical surroundings for the viewing of photographs by witnesses;
- (e) lack of apparent "standard procedures" for handling witnesses viewing suspect photographs;
- (f) the individual witness's own inability to concentrate on more than a small number of books before all the photographs take on similarities;
- (g) the high cost of production, display and storage;
- (h) poor categorisation which requires the witness to view more photos than may be necessary.

3.4.6 Microfilming Photographs

Plans are now underway for police photographs to go on microfiche. This has several advantages to the privacy of the individual in that more specific groupings, can be shown rather than large books and thereby fewer persons' photographs will be shown. However, it may result in the creation of not just local, but complete sets of photographs for each Police station. The increased availability of a greater portion of these records could accentuate their importance as privacy intrusions.

The increased effectiveness of the photograph record system would appear necessary before any expansion is envisaged. The fact that a person's photograph is more readily recognised by a witness than a fingerprint, makes the privacy danger posed by the photograph more immediate, especially if the person recognised is not being sought by Police. For this reason the Committee cautions against any major increase in the use of photographic records systems without more adequate privacy safeguards. However, at this stage it makes no recommendations in this regard.

CHAPTER 4: DATA SECURITY - PHYSICAL SECURITY AND ACCESS TO DATA

4.1 Data

The records which comprise the Criminal Record Office are set out in para. 2.2.

4.2 Central Fingerprint Bureau of Australia

It is important to remember that the CRO is the recording section for the Central Fingerprint Bureau of Australia and that any record here could be duplicated within any bureau of any other law enforcement agency.

4.3 Data Security - Physical

No entry to the building can be obtained without the production of an authorisation certificate. Physical access to the Criminal Records Office is limited to the staff of that Office and to selected members of the CIB squads. From the brief examination by the Committee the physical security appears adequate.

4.4 Accesses

4.4.1 There are basically five types of accesses:

- (a) CRO staff and selected members of CIB squads (see para. 4.3);
- (b) Police generally and certain law enforcement agencies; (1)
(para. 4.3)
- (c) the Public Sector; (see para. 4.5.2)
- (d) the public through voluntary disclosures (see para. 4.8);
- (e) individuals to their own records (see para. 4.9).

Many government departments, statutory bodies and the courts obtain information from the CRO. For full details and discussion see the Committee's discussion paper "The Use of Criminal Records in the Public Sector" BP 41 November 1977.

4.4.2 Accesses by Police and Certain Law Enforcement Agencies

These obtain information either by attending at the counter in person, by written report, by telephone or by telex.

4.4.3 The N.S.W. Police

Officers are permitted to access CRO for location and identification. Usually the full name and date of birth is supplied by the officer. The officer specifies the purpose of the enquiry when requesting the information, e.g. that the person has been charged or is suspect, or is applying for bail, or that the photo reference is required, etc. For Courts of Petty Sessions' purposes the photostat or typed duplicate of the record is supplied. If a Police Officer applies personally he only sights the record. Telephone enquiries are answered verbally.

(1) Police Forces of other States, Commonwealth Police, Customs Officers, Corporate Affairs Commission N.S.W. Investigators, etc. (the latter two examples gain the data indirectly through seconded Police Officers.)

4.4.4 Authority for the Access

A serving member of the N.S.W. Police Force has merely to be identified as such and the reasons for the enquiry established to be given access.

4.4.5 Access to Courts

The only known authority for the production of criminal record information is given by s413 of the Crimes Act which provides for the production of "a document purporting to be a record of conviction of the accused person for the offence purporting to be signed by the authorised officer shall be received in the (Court) proceedings as evidence of that fact". Such an authorised person may be "the officer in charge of the Central Fingerprints Bureau of the Police Department or any person authorised by him for the purposes of this section".

4.5 Logging of Accesses

4.5.1 Telephone Enquiries

These are recorded on a form (Appendix 7) Before any information is given the caller must give his registered police number if he is a policeman and verified by the police seniority list. If he is not a police officer he is identified as an authorised enquirer. Such logging information is filed in date order and maintained for twelve months.

4.5.2 Written Enquiries

A copy of all replies are kept and retained in date order, grouped according to the various enquirers. (See BP 41 for details of authorised enquirers (BP 41 - Privacy Committee "The Use of Criminal Records in the Public Sector))

4.6 Frequency of Access

Police enquiries comprise approximately 250,000 per annum made up of

- arrests calculated from fingerprints received 90,000 p.a.
- Police enquiries (at 400 per day) 146,000 p.a.
- telex messages 12,300 p.a.

4.7 Unauthorised Access to the CRO

4.7.1 In any discussion of the security of criminal record information within the CRO it is necessary to confront the problem of unauthorised access and to discuss certain measures for its prevention.

4.7.2 Employers, private investigators, etc. often say that they have access to CRO to check prospective employees, employees suspected of theft, etc. Similarly, people complain to the Committee about refusal of or dismissal from employment, and insurance problems, because of disclosure of their records. Police, however, admit that unauthorised accesses do occur.

Six methods of unauthorised access seem possible:

- (i) by a public servant or Police Officer who works in CRO itself;
- (ii) by a CIB officer who has authority to personally search CRO records;
- (iii) by a local Police Officer obtaining a record by telephone;
- (iv) by an employee of another department which has telephone access to CRO obtaining a record by telephone (Corrective Services, YCS, Probation, etc.);
- (v) by an employee of a body which has written lists name checked (for a list of bodies see BP 41) adding a name to that list;
- (vi) by a third party who knows the procedures in (iii) or (iv) ringing CRO direct.

4.7.3 Present Security Practices

Each of these situations requires different security measures. The present practices relevant to the maintenance of such data security are as follows:

- (a) CRO employees: Besides careful staff selection and supervision and investigation of complaints, no particular security measures are imposed on this group. Logging of all staff accesses is considered impractical.
- (b) Searches by CIB Officers: Selected members of the CIB squads are authorised to enter the CRO and search the records themselves. Such accesses are always made with the knowledge of a Sergeant at the CRO.
- (c) Local Police Telephone Checks: Any Police Officer can obtain record details by telephone on providing the following information: name; rank; station; registered Police number; badge number. CRO staff record these details in a daily log book, check the given Police number against the Police seniority list, and also write "yes" in the log book if the person enquired about did have a record. No entry is made on the person's CRO card to say that it has been accessed. CRO gives out records on incoming calls and does not insist on ringing back. The enquiry logs are kept for 12 months, filed in date order.
- (d) Other Departments with Telephone Access: Youth & Community Services, the Probation and Parole Board and the Department of Corrective Services (prisons section) each have one appointed liaison officer who obtains CRO information, sometimes by telephone, but often by coming into CRO. All enquiries are logged in the usual log book and are only dealt with by a Sergeant and not by clerical staff. The name of a person's Probation Officer is rarely included on the CRO card. Therefore the Probation and Parole liaison officer collects a weekly list of probationers/parolees who have been charged again, for distribution to their Probation and Parole officers.
- (e) Bodies Doing Written Name Checks: Name checks must be requested in writing on the official letterhead of the body and must be signed by the officer authorised by the Police to request such checks. (One at any given time.) Results would be collected by the authorised officers or sent to the department's official address.

The CRO retains a duplicate of the replies given to Department/authority requests for criminal record information, filed under the name of the Department/authority in date order for 12 months from the date that the check is made on the CRO card. Where urgent telephone enquiries are made, they are dealt with by a sergeant and later confirmed in writing.

- (f) Third parties ringing the CRO direct: Any person knowing the procedure in (iii) or (iv) and the necessary details could obtain a person's record from the CRO by using any normal telephone.

The "Police Regulation Act" s17(1)(c) creates the offence of assuming "the name, designation or description of a member of the Police Force or of any class of such members". The penalty for such an offence is a fine of \$200 and/or imprisonment for up to six months.

4.7.4 Removal of Card

Where there is a suggestion of possible unauthorised access, the officer in charge may remove the card from general access for an appropriate period to allow for detailed supervision of every request.

4.7.5 Possible Reforms to the Present Security Check System

- (a) Improvement in Logging of Accesses: It seems that all external accesses, both Police and non-Police, and whether in person, by telephone, or in writing, are supposed to be logged, and with few exceptions would be. However, the logs are only kept in date order, with no notation being made on the CRO card that it has been accessed. Therefore, in order to know if a particular CRO card had been externally accessed, you have to either know approximately when the access occurred or search back through all the logs (over 450,000 p.a.).

The Committee's investigations of complaints which allege some form of unauthorised access, would be facilitated if the record card was noted with an access code and the date when it was accessed. This could be done in the blank space on the front of the card (Appendix 3). Two different access codes could be used, one for accesses recorded in the daily log book (oral or telephone) and the other for those resulting from a written enquiry to make retrieval easier.

Proposal (2)

That the present practice of logging accesses on a daily basis be expanded by noting on the card the date of access and whether the access was oral or written.

- (b) Ring-Back: The major defect in the existing system is that any person knowing the system and a serving Officer's Police number could ring from any telephone and obtain information from clerical staff. This is particularly vulnerable to ex-Police or anyone who can convince a Police Officer to explain the system.

This problem may be largely removed by a ring-back system. However, the necessity for a quick and relatively uncomplicated system for the recovery and supply of criminal record information may outweigh the security advantages of such a system.

The ring-back system would involve the following:

- (i) no information would be given on incoming calls;
- (ii) the caller would give his station and phone number and the return call would only be made where the number was verified as being that of the station (calls from other than police stations would only be handled by a CRO sergeant);
- (iii) the caller would give his name and police number and the call back would only be to him (thus reducing the danger of one officer using another's name to avoid detection).

Such a system, if initiated by the CRO, would cost more than \$14,000 per annum in telephone calls and this cost factor would be greatly increased if extra staff were required to operate the "ring back" and compensate for the time lost in such a system. In 1973-74 the CRO attempted a "ring back" system to improve security but found it was considered to be unsatisfactory by most officers. Once telephone contact is broken, all phones at the CRO may become busy. Also the phone at the station end may be engaged when the CRO rings back.

Proposal (3)

Unless the incidence of unauthorised access becomes such as to warrant the introduction of a ring-back system on a permanent basis (despite the difficulties) the Committee would support the continuance of the current CRO practice of only randomly accepting calls on a ring back basis for a few hours.

- (c) Spot Checks: Perhaps a more detailed and less defective form of checking system would be as follows:

Internal Affairs or CRO senior officers should conduct periodic spot checks of a random sample of CRO checks either in the form of previously logged calls or incoming calls to ensure that the check was made by the Police Officer stated, and that the purpose stated was legitimate. It may be considered necessary to do these checks on a face-to-face basis so as to overcome the difficulties of telephone checking and further test the accuracy of reasons given. The irregular nature of these checks may of itself add to the effectiveness of the method as a deterrent to unauthorised access.

To add to the accuracy and overcome the suggestion that "any officer worth his salt" would have little difficulty in giving reasons for a CRO enquiry, wherever possible, the check should also be verified with the subject of the card access.

Proposal (4)

The Committee recommends the implementation of random checks of requests for information verified wherever possible with the subject of the enquiry.

The frequency of the checks could be varied to correspond with the incidence of complaints or what the officer in charge of the CRO considers to be the security needs at that time.

- (d) Security of Computerised Data: For the Committee's recommendations regarding data security as it relates to computerised records in particular, see chapter 7.
- (e) Increased Penalties: At present, the penalties associated with illegal accesses seem to be inadequate in 3 ways:
 - (i) the penalty under the Police Regulations Act for improper disclosure of a criminal record by a Police Officer or Public Servant is a fine between \$10-\$40. Note: such a disclosure also constitutes a breach of discipline which might lead to the dismissal of the Police Officer or Public Servant concerned;
 - (ii) third parties impersonating Police Officers (or others) to obtain CRO information may only incur a \$28 fine under the Police Regulations Act s17(1)(c) or a penalty of \$200 under s171(e) of that Act;
 - (iii) third parties colluding with Police to obtain information from CRO may incur a fine under s17(1)(d) of \$200. Both Police Officers and public servants working at the CRO or Police stations may be liable for disciplinary sanctions under the Police Regulations or the Public Service Act respectively. These latter sanctions would appear to be the more severe by far.

Proposal (5)

That maximum penalties for illegal accesses be increased to \$2,000 or one month in prison.

4.8 Voluntary Disclosure by Police

- 4.8.1 Situations may arise where local or investigating Police volunteer information about a person's criminal record to someone they consider should be availed of such information, e.g. his employer, the management of a club in which he is a member, etc.
- 4.8.2 Under the heading of "secrecy regarding Police Business" (Section XVIII of the Police Rules) the following policy statement is made:
 - "1. Police will observe the strictest secrecy in regard to Departmental business, and are forbidden to communicate without official authority in any way whatever to any person outside the Force any information in regard to Police or other official public business connected with their duties, or which may come to their knowledge in the performance of them.
 - 2. Police will not, unless authorised, give any information to persons outside the Force concerning any reports or records of accidents, convictions, or other occurrences, nor is any such person to be shown such reports, etc.

Persons asking for such information are to be civilly referred to the Superintendent-in-Charge, or the Officer-in-Charge of the Division or Sub-district, who may, if the person is interested in the matter, give such information as he considers desirable; ... (emphasis added).

The matter is further discussed in Police Instructions No. 39 "Miscellaneous":

- "9. Police must exercise every care that they do not interfere with discharged prisoners and prevent them from earning a decent and honest livelihood.

It must be remembered that once a prisoner has served his sentence he has the same rights as any other citizen with regard to employment, and if Police go out of their way to inform persons giving employment to a discharged prisoner of his previous history it may have a very detrimental effect, and, indeed, may be the means of his becoming a hardened criminal.

On the other hand, of course, it may be necessary under some circumstances to inform employers of the character of persons employed by them: but in no case should this be done without reference to headquarters." (emphasis added)

- 4.8.3 The Rules are made under the Police Regulation Act 1899, s12. Breach of a Rule would seem to lay an Officer open to internal disciplinary proceedings, but would not in itself be an offence, except against s14 of the Act which provides penalties of between \$10 and \$40.

S17(1)(d) of that Act also makes it an offence for third parties to collude with Police to obtain such information (\$200 fine).

- 4.8.4 The Committee supports the existing policy in the Police Rules (Section XVIII, Rules 1 and 2) and Instructions (No. 30, paragraph 9) which provide that Police should not disclose a person's criminal record to any person outside the Police Force without obtaining approval from a designated senior officer (or headquarters), but considers that the policy needs clarification to allow it to be effectively enforced.

Proposal (6)

The Police Rules should be amended to provide that:

- (i) A Police Officer should not make such a disclosure of his own accord unless he reasonably considers that to fail to do so would place another person in an immediate and serious risk.
- (ii) In other instances he should report the circumstances to a senior officer of the rank of Inspector or above who should make the decisions whether, and how, the information should be disclosed.
- (iii) In both cases the disclosure, and the reasons for it, should be recorded in a central log book which should be periodically reviewed by the Police Commissioner.
- (iv) The person whose record has been disclosed should be informed in writing of the disclosure and given the opportunity of perusing the summary of the report or having it examined by an appropriate third party.

This should ensure that the discretion to disclose is exercised in a responsible way.

Proposal (7)

There should be similar offences and penalties for unauthorised disclosures other than those proposed in proposal (6) to those proposed for illegal accesses in proposal (5).

4.9 Individual Access

- 4.9.1 There are three methods by which an individual may gain access to his own criminal record:
- (a) when charged, it is made available to the individual or his legal representative on request;
 - (b) through the agreement arranged between the Police Department and the Privacy Committee where a person may have his fingerprints taken at Police headquarters (to establish identity) and a fee of \$10 is paid. The results of all court appearances substantiated by fingerprints are supplied. The copy is marked to state that it is only supplied for the applicant's information and for no other purposes and that any abuses of this information should be exposed by the Privacy Committee (see chapter 6 for details);
 - (c) by the issue of a subpoena Duces Tecum for the production of the record at the court named therein.
- 4.9.2 Only particulars of arrests, charges and court appearances are supplied. The information recorded on the front of the record card is not supplied (Appendix 3).
- 4.9.3 Following discussions with the Police Department in late 1975, a procedure was established in March 1976 whereby members of the public could apply for a copy of criminal record information relevant to them and held by CRO in order to ascertain its contents and verify its accuracy.

While the CRO appears to maintain a very high standard of accuracy, there will always be human error within the CRO as well as from the Courts, original and appeal, and other sources of data throughout Australia and overseas.

Any person can apply to any Police Station for a copy of his criminal record. He will be required to pay a fee of ten dollars (\$10) and have his fingerprints taken to verify his identity.

A written reply is sent direct to the applicant. If the search has not disclosed any record the letter will state this. If the search has disclosed a record, the letter will ask the applicant to attend the place where the application was lodged. After this letter has been produced, and signatures compared, a copy of the criminal history section of the CRO card will be made available (i.e. all court appearances and the results of such appearances). Matters of criminal intelligence are not supplied.

The record will include matters arising from court appearances in all States and territories and under Commonwealth law.

So as to make applicants aware of the reason for the supply of copies of records, and to guard against possible misuses of the procedure, each record copy is to be endorsed with the following statement:

"This information is given to you solely for the purpose of your verifying the accuracy of the information contained herein.

It should not be requested to be produced by any person for employment applications or any other purpose.

Any attempted or actual misuse of this information should be reported to -

The Executive Member,
Privacy Committee,
G.P.O. Box 6,
SYDNEY. 2001

Telephone: 238 7713."

- 4.9.4 Although the Commissioner originally agreed to provide a photo copy of the court appearances side of the CRO card (as stated in para. 1.1) (1), this is not the current practice. Rather, the court appearance details are typed verbatim onto a form similar to the antecedents form prepared for the court (Appendix 2). This method has the advantages of the notation "This information is not a true record unless this form is in its entirety. Last entry recorded is (date)." This is to prevent a person presenting part of his record as the complete record. As well as this protection, the fact that a typed transcript is an original makes it more difficult to tamper with, than would be the case with a copy (particularly if it bore on its face "This document is an original copy with no alterations or erasures").
- 4.9.5 However, a photocopy has the advantage that the applicant can be more confident that he is being given a copy of his complete record just as it appears on Police files. If photocopies were made onto sheets larger than CRO cards, the same warnings as are now typed onto the antecedents form could be typed onto the photocopy. There would be a considerable reduction in typing cost and time taken in the preparation of records if photocopies were used in preference to transcripts.
- 4.9.6 The present agreement between the Police and the Committee is that only the data on the "court appearances" side of the CRO card should be divulged to the applicant. Police intelligence information would otherwise be disclosed. The only information presently given out for non-Police purposes is that on the "court appearances" side.

Arguments in favour of the provision of full copies of CRO cards are as follows:-

- (a) the CRO should be regarded as an administrative record system, separate from intelligence. A clear separation between the two types of records is necessary for the different access and security rules appropriate to each to be applied.
- (b) At present there seems to be little on CRO files which would genuinely constitute intelligence information such that individual access to it could jeopardise law enforcement or allow a criminal to avoid detection in future. In the few cases where this might occur, any rule could allow an exception to be made. The main items which could be argued to constitute "intelligence" are:
 - (i) identifying characteristics - might assist changes in appearance;
 - (ii) aliases -(i.e. names given on arrest) might assist a criminal to know what names he can safely give Police if he wants to get bail, etc;
 - (iii) arrest details - disclosing names of arresting Police;
 - (iv) fingerprint classifications, photo numbers, and old Police Gazette references seem of little danger.

(1) Letter from Commissioner of Police to Executive Member of Privacy Committee dated 18 March 1978.

- (v) wanted (for arrest/questioning) details are not dangerous either: if still current, Police should be pleased to tell the person about them. If no longer current, then the person will have either been arrested or questioned, or could legitimately ask why Police then wished to contact him;
- (vi) if the dates of all accesses are logged on the CRO card as suggested (see 3.1(c)(i) above), then a copy of the CRO card would tell a person how often his card had been accessed, and whether such was a Police or non-Police access. While there should be no objection to people knowing of all non-Police accesses to their files (so they can check for abuse), there may be objection to their knowing of all Police accesses (e.g. to find out if they were suspected of a crime even though never approached by Police - and therefore whether it was safe for them to commit further similar crimes). Note: the same could be argued in (v) above.

4.9.7 The problems raised by (ii), (iv) and (vi) in para 1.5(b) probably preclude the provision of the complete CRO card data. Most of the information is used primarily for Police purposes and therefore the provision of total access to all data by the individual is not crucial. However individuals should be able to request details of all non-law enforcement agencies' accesses to their files and have all law enforcement accesses checked as to the bona fides of the enquirer.

Proposal (8)

- (a) *The existing procedure (para. 4.9.3) by which a person can obtain a copy of the Court appearances as part of his CRO card, should be followed. (It is not proposed that it be extended to cover any other matters recorded on the CRO card.)*
- (b) *A photocopy of the court appearances section should be given to the person rather than a typed transcript (as is currently done). This photocopy should have typed on it in red (as on the current transcripts) "This information is not a true record unless this form is in its entirety. It comprises () pages and the last entry recorded is (date)".*
- (c) *The warning about improper demands by employers, insurance companies, etc. to produce a copy of the record should be expanded, as previously agreed by the Police, to also state: "Any attempted or actual misuse of this information should be reported to the Executive Member, Privacy Committee, Box 6, G.P.O., Sydney, telephone 238 7713.*

4.9.8 Traffic Offences

Most convictions for traffic offences (unless serious) are not recorded by the Police Department but are recorded by the Department of Motor Transport.

For a fee of \$1.50 any person can obtain a photocopy of his traffic conviction record. A driver's licence or other proof of identity, together with full details of the licence, must be provided. The record will only be sent to the address recorded on the licence.

CHAPTER 5: RETENTION

5.1 Present Practices

5.1.1 Destruction or Archiving. The only automatic destruction procedure currently practised by the CRO relates to records of persons born prior to 1881. There is also the procedure for the destruction of fingerprints and photographs. This procedure is dependent on an exercise of the Commissioner's discretion (para. 5.2.5).

5.1.2 Need for Retention of Police Records. Police records are maintained for both Police and non-Police purposes. The non-police uses to which this data is put are extensively examined in Privacy Committee BP 41, 1977.

5.1.3 The major police purposes are as follows:

- (a) the detection of crime
- (b) apprehension of offenders
- (c) establishing the identity of arrested persons
- (d) locating and identifying missing persons
- (e) locating and identifying subjects of warrants
- (f) establishing previous criminal history of the individual and provision of such information to the courts for sentencing and bail determinations
- (g) assist interstate and overseas police forces in their investigations
- (h) internal intelligence purposes.

This list is by no means exhaustive and several of the categories clearly overlap. However, from these purposes, it is obvious that it is necessary for some record system of criminal data to be maintained if a Police Force, such as that which exists in this State, is to function effectively.

5.1.4 The Police have expressed the view that, all records maintained by them (with certain discretionary exceptions) should be complete and permanent as they are required for Police purposes.

Rather than agreeing with the destruction of criminal record information as the ultimate privacy protection, the Police are of the opinion that the disadvantages caused by the loss of such data would outweigh the benefits to the privacy of the individual. The volume and variety of information which they maintain and the frequency of duplication of this information throughout the Department would make the comprehensive destruction of any data administratively difficult.

The protections presently existing in the Police criminal record system such as security of access and restrictions on disclosure, are discussed in Chapter 4 and their limitations are examined.

5.2 Unsuccessful Charges

5.2.1 An unsuccessful charge leaves 5 records which require consideration:

- (a) fingerprints taken;
- (b) photographs taken;

- (c) the court appearance details leading to dismissal, successful appeal (back side of CRO card);
- (d) the arrest details (front side of CRO card);
- (e) the existence of the CRO card and strip index cards which of themselves reveal that the subject has come under Police attention.

Other records may exist e.g. Policeman's notebook, records of interview, charge sheets, court records, etc., but records (a) to (e) are the ones that are centrally indexed and hence more easily accessed.

5.2.2 Fingerprints and Photographs

The basic reasons for supporting the maintenance of all fingerprint records, including those associated with dismissed charges, relate to the need for complete records and a central locator for missing or unidentified persons.

The Crime Intelligence Unit might also want to retain both prints for future intelligence purposes, e.g. where a person was acquitted of a serious offence on a technicality, or a person whom Police believed to be continually involved in crime but who had not previously been photographed or fingerprinted.

5.2.3 Court Appearance and Arrest Details.

It is important that if arrest details are to be recorded at the CRO, then dispositions should accompany them. If details of dismissed charges and the court appearances leading up to them are to be considered for deletion, then the arrest from which they arose should also be deleted.

Certain arguments against any suggestion of deletion are:

- (a) accepting that a considerable number of people are acquitted when in fact guilty records of dismissed charges can often be quite valuable to police in deciding whether a person is a suspect for a subsequent crime.

In reply it can be said that the CRO is a repository of factual data concerning crimes. If the Court has determined that a person was not guilty of a charge, then no centralised record of the charge should be kept. It is for the Police to ensure that crimes are accounted for, and not to associate an acquitted person with conviction data purely because they are not satisfied with the court's determination.

- (b) Provided dismissed charges are not used for employment, licensing, etc., are not made available to courts for sentencing purposes, and are kept under adequate security they are not a great danger to the privacy of the individual.

The risk of unauthorised access might well outweigh the value of those records for the proper police function of investigating crime.

Why should any centrally recorded information (with its inherent dangers of unauthorised or unnecessary authorised accesses) be maintained when the subject has been acquitted?

- (c) The dismissal record provides conveniently available permanent evidence of the proceedings for which the person was acquitted. He may require such evidence at a later date. Therefore it ought to be destroyed only at the request of the individual, if at all.

This type of argument must be balanced against the fact that sufficient information for the purposes of answering correspondence can be obtained from court papers and non-indexed Police files. Likewise, court papers will provide all necessary information of the acquittal for the subject's purposes. (Problems are unlikely to arise with the eventual destruction of court papers).

- (d) The arrest or dismissal details may later be needed by Police, if, for example, a Police officer was sued or correspondence about the case had to be answered. This is of particular significance within the first year or so from the date of the dismissal.

Much the same response might be used for this argument as was raised in (c) above. At best, this could only justify a limited retention of the records.

- (e) On the existing manual card system deletion would take the form of obliteration of details of the particular entry from the face of the card, unless destruction or re-writing of the whole card was contemplated.

Although deletion in a manual system might prove difficult initially, such difficulty will diminish as the Department moves towards computerisation of its records.

5.2.4 Intelligence Requirements.

Where police wish to keep certain details of dismissed charges for intelligence purposes, they should be maintained in the separate, more secure, intelligence file system, rather than in the present universal retention system. There may even be justification for a requirement that information as to dismissed charges should only be maintained for intelligence purposes with the agreement of a magistrate. However this may be imposing too great a restriction on the maintenance of files, the purpose and function of which rests very much with the discretion of the Police Department and which rely on anonymity for their effectiveness.

The Committee would envisage that the need for the retention of information concerning dismissed charges for intelligence purposes would not be great. It is envisaged that the bulk of such data should not be transferred from the CRO to the Crime Intelligence Unit records rather than destroying it.

5.2.5 Destruction on Request.

If a person is fingerprinted or photographed in the process of being charged with an offence and the offence is not subsequently found proven (either because he was acquitted or the conviction was upset by an appeal or because the charge was not proceeded with), then he can apply to the Commissioner of Police for the destruction of such fingerprints and photographs.

Although the law does not require the Commissioner to accede to such applications, he has advised the Committee that he exercises his discretion to customarily consent to such applications. The Committee has not received any complaints that a request has been refused.

The destruction is limited to the sets of fingerprints or photographs taken specifically in relation to the particular charge which was not found proven and does not apply to any charges where such facts were found proven.

The destruction of fingerprints or photographs does not mean that the Police Department retains no record of the charge. A card is maintained in the CRO office, stating details of the court proceedings and that fingerprints or photographs have been destroyed on application. The record cards are retained on file because current departmental policy dictates that such material forms an integral part of Police records and intelligence and should remain intact for future reference. Also some duplication of the criminal record may be found in the MO section, where it might be manually recorded, recorded on microfilm or computerised. Full details of the charge and the result would be contained in the relevant charge book at the Police station where the person was initially charged (see para. 5.2.1).

Rarely is the discretion used to allow destruction of fingerprints and photographs when the charge was dealt with pursuant to s556A of the Crimes Act or s83(3) of the Child Welfare Act as the facts were found proved and the record is needed for future sentencing purposes.

5.2.6 The Australian Law Reform Commission in its criminal investigations study recommended (1) that:

"the police power to take fingerprints, photographs, handwriting samples, and the like, should be limited to situations where the obtaining of such fingerprints, etc. is reasonably believed to be necessary for the identification of the person in relation to the offence for which he is in custody or where a magistrates' order has been obtained. (para 113-115)

Prints, photographs and samples taken in connection with an offence which is not found by a court to be proved or which is not proceeded with, should be destroyed. It should be an offence for a police officer or other person to make a copy of any prints, etc. required to be destroyed in this way (para 116)".

Clause 70 of the Criminal Investigation Bill 1977 (Commonwealth) provides that where proceedings are not instituted or the court does not convict the individual or finds without recording a conviction, the commissioner shall cause the relevant prints, recordings, photographs or samples to be destroyed within 12 months of their collection or an extended period, where so ordered by a magistrate (see clause 71). This Bill has now lapsed.

Therefore in respect of fingerprints and photographs, the ALRC would agree with the current practice in N.S.W. as to the destruction of such prints and photographs where charges are not successful (not so for s556A determinations) except that it would remove the Commissioner's discretion and make such destruction mandatory within 12 months, unless there is a magistrate's order to the contrary.

(1) ALRC-Criminal Investigations Report 1975, p. 148, para. 335-6

5.2.7 Practicality of Destruction

It would be practical for the CRO to simply advise the fingerprint bureau when it receives the dismissal details. Both administrative convenience and financial economies would be better effected when CRO and Central Fingerprint Bureau records are computerised.

The destruction of photographs may pose more difficulties than the simple destruction of fingerprints. Photographs are distributed to local stations on request. However these local stations could be instructed not to request such photos until the charge had been determined, or, if they considered it necessary to have a photo during the charge period, be told later to remove the photo from photograph books following the dismissal of the charge. With the advent of microfiche, the removal of individual photos may be even more difficult. It might be necessary to remove the person's name from the proposed microfiche name index which would make specific access possible but would not overcome recognition during perusal.

Special Branch: In its report on the Special Branch of the N.S.W. Police Force (Privacy Committee BP44 March 1978, para. 4.3.3 and 7.5.5) the Committee noted that if the Commissioner consents to destruction then any copies held by Special Branch should also be destroyed.

5.2.8 Automatic Destruction on Dismissal

The Committee accepts the view that the CRO should not retain details of charges which the court has dismissed.

Proposal (9)

- (a) *Subject to (b) hereof, arrest and court appearance details relating to unsuccessful charges should be automatically deleted from the records of the Criminal Records Office following the court's determination (note: para. 5.2.1). The subject's name should be removed from the strip index if such data is the sole entry on the card; and the card should be destroyed.*
- (b) *Prior to any deletion or destruction of such arrest and court appearance records, the Commissioner of Police may, on the basis of public safety, apply to a magistrate for an order allowing the retention of such information for a period not exceeding 10 years.*
- (c) *This proposal should not be automatically applied retrospectively (see para. 5.8).*

5.3 Section 579 Crimes Act

5.3.1 Old Offences: S579⁽¹⁾ provides that whenever a person is placed on a recognizance (pursuant to s554 substituted sentence, s558 deferred sentence of s556A(1)(b)) then if he has not breached the terms of the recognizance, or had any offences proven against him (indictable or punishable by imprisonment) during a fifteen year period after the recognizance was entered into, the conviction or finding shall be "disregarded for all purposes whatsoever" and "be inadmissible in any criminal, civil, or other legal proceeding as no longer being of any legal force or effect". This includes the restriction of such details from "any application for a licence, registration, authority, permit or the like under any statute".

5.3.2 Practical Operation of s579: The Police Commissioner may, on application destroy fingerprints for any offence coming under s579, and consent to the noting on the CRO card of a prohibition from disclosing the offence on any enquiry (2). The CRO may not disclose details of recognizances which are outside the 15 year

(1) S579 - see following page

(2) see page 28

period stipulated under s579 where there has been no intervening offence (if so noted). This is the policy, whether or not the individual makes application to the Commissioner. The non-disclosure is automatic. However, the Committee has seen instances where such data has been inadvertently given out, because the card did not bear the notation as to the effect of s579.

- (1) S579: "(1) Where, following the conviction of any person for an offence or a finding that a charge of an offence has been proved against any person, whether the conviction or finding was before or after the commencement of the Crimes (Amendment) Act, 1961 -
- (a) sentence in respect of the conviction was suspended or deferred upon the person entering into a recognizance or, in substitution for sentence in respect of the conviction, the person was required to enter into a recognizance, or no conviction in respect the finding was made and the person was discharged conditionally on his entering into a recognizance; and
 - (b) a period of fifteen years has elapsed since the recognizance was entered into -
 - (i) without the recognizance having been forfeited during that period or a court having found during that period that the person failed to observe any conditions of the recognizance; and
 - (ii) without the person having, during that period, been convicted of an indictable offence on indictment or otherwise or of any other offence punishable by imprisonment (otherwise than under s82 of the Justices Act, 1902, as amended by subsequent Acts) or without a finding during that period that a charge of such an indictable or other offence has been proved against the person,
- the conviction or finding shall, where that period expired before the commencement of the Crimes (Amendment) Act, 1961, as on and from that commencement, or, where that period expires or has expired after that commencement, as on and from the expiration of that period -
- (c) be disregarded for all purposes whatsoever; and
 - (d) without prejudice to the generality of paragraph (c), be inadmissible in any criminal, civil or other legal proceedings as being no longer of any legal force or effect.

Without prejudice to the generality of the foregoing provisions of this section, any question asked of or concerning that person in or in relation to any criminal, civil or other legal proceedings otherwise than by his counsel, attorney or agent or other person acting on his behalf may be answered as if the conviction or finding had never taken place or the recognizance had never been entered into.

- (2) Notwithstanding the provisions of subsection (1), where in any criminal, civil or other legal proceedings the person first referred to in that subsection, by himself, his counsel, attorney or agent or other person acting on his behalf, otherwise than in answer to a question that can, in accordance with the last paragraph of that subsection, be answered in the negative, makes an assertion that denies the fact that the conviction or finding took place or that the recognizance was entered into, then the conviction, finding or recognizance is admissible -
- (a) in those proceedings, as to the character credit or reputation of the person so referred to;
 - (b) in any prosecution for perjury or false swearing founded on the assertion.

- 5.3.3 Disadvantages of s579. The defects inherent in a provision such as s579 are obvious. For the types of offences (and sentences imposed) that it is intended to cover, 15 years seems to be a disproportionately long period before the provision takes effect. The section is limited to offences for which the court imposed recognizances and has no operation in many minor offences which the court may have dealt with by a fine, a s556A(1)(a) dismissal, or a "rising of the court" order, or where a monetary recognizance may have been forfeited for want of an appearance. The protection of the section is forfeited if, at a later date, the court finds that the facts of any charge are proved and imposes a conviction or applies s556A for such a charge. The charge would relate to any offence, no matter how minor which is punishable by imprisonment and which arises during the 15 year period. The statement that a conviction satisfying the provisions of s579 shall be disregarded for "all purposes whatsoever" is unclear.

The Committee in its BP41 recommended that all government and statutory bodies should primarily limit their questioning to convictions which occurred in the previous 10 years and this would effectively exclude from questioning any convictions which might be subject to s579. The general restriction at the time of the writing of this report has been accepted by the majority of users including the Public Service Board, the Public Transport Commission, the Department of Motor Transport (for licensing) and most licensing bodies.

5.3.4 Comments on s579

- (a) This section does not apply to section 556A dismissals, fines and sentencing to the rising of the court. The Committee feels that it would be reasonable after the affluxion of the 10 year period referred to in this chapter that the section be amended to include all charges which have been dealt with under s556A, including dismissals.
- (b) The Committee also considers that after a period of 10 years a person should be able to apply to a magistrate to have the benefit of s579 applied to a particular conviction notwithstanding specific minor offences which may have occurred in the intervening period. This would give s579 a realistic degree of flexibility.
- (c) To be consistent with its overall proposals the Committee considers that the period after which the benefits of s579 becomes available should be reduced from 15 years to 10 years.
- (d) For the proposals as to culling of entries dealt with pursuant to s579 see Proposal (11).

- 1) cont. The non-disclosure of the conviction, finding or recognizance in the making or giving of a statement or evidence as to the good character, credit or reputation of the person so referred to shall not of itself be taken, for the purposes of this subsection, to mean that the statement or evidence contains such an assertion.
- (3) In this section "legal proceedings" includes any application for a licence, registration, authority, permit or the like under any statute.
 - (4) This section does not affect the operation of section 55 of the Defamation Act, 1974, or the operation of section 23 of the Evidence Act, 1898, for the purposes of section 55 of the Defamation Act, 1974.
- (2) Such a prohibition may not be seen to apply to antecedent reports to Courts or enquiries made by investigating Police. Under the section it would appear that the prohibition should also cover these areas.

Proposal (10)

- (a) *s579 of the Crimes Act should be amended by reducing the period of 15 years referred to therein to 10 years.*
- (b) *The provisions of the said s579 should be extended to apply to offences where the provisions of s556A(1)(a) applies, a fine was imposed or the person was sentenced to the rising of the court.*
- (c) *The said s579 should further be amended to provide that a person whose record would come under the provisions of s579 except for the occurrence of subsequent charges should be able to make application to a magistrate for an order that the benefits of s579 should apply to specific records more than 10 years old despite intervening minor offences.*

5.4 The Culling Programme

5.4.1 The "Red Tick" Cull

This programme was commenced early in 1970 and was completed some 3 years later. Over that period approximately 125,000 cards were removed from the central card index and the corresponding subject names were taken from the strip index. On extraction the cards were indexed, microfilmed and stored separately from the current manual system.

The criteria used for inclusion in this particular "cull" are as follows:

- (1) For court appearances prior to 1960:
 - * persons with only one entry who have been arrested for any offence with the following results:
 - dismissed - discharged - no evidence to offer - acquitted, etc.(This would cover most offences effected by s579.)
 - * persons with only several minor convictions, offensive or indecent language, offensive behaviour, traffic offences, street offences, minor stealing, driving under the influence, etc.
- (2) All notations of licences not renewed for the last 3 years.
- (3) Cards marked "deceased".
- (4) Cards marked "deported".
- (5) Cards with subjects who were born prior to 1901.

In March 1978 the Commissioner of Police gave a direction that no internal or external accesses should be given to data given "red tick" status, unless specifically authorised by the officer in charge of the CRO. In practice it would appear that the access of this data is a little more routine than suggested by the directive. If a person is re-arrested and his fingerprints correspond with sets held at the central fingerprint index, the "red tick" index will be checked if his name is not on the strip index nor his card in the CCI.

In a situation where such a subject comes under notice, after having his card culled, the original data will be restored to card form and returned to active storage.

Since the completion of the red tick cull programme, cards have been restored to the CCI (a restoration rate of approximately 1% of the total number of cards culled).

5.4.2 The "Black Tick" Cull

A second programme of removal and microfilming of cards has been recently completed. The criteria for this programme were far more general than those mentioned in 5.4.1 and the "cut-off" year for the most recent notation on the card was raised to 1965. This cull took out over 250,000 cards. However, the CRO treats this cull as more an exercise in using storage facilities to better advantage, rather than an effort to restrict the accessibility of the data involved.

The restoration rate for this programme is many times greater than is the case with the earlier cull.

- 5.4.3 The Committee considers that the experiments presently being carried out by the CRO in respect of culling are both an encouraging and responsible attempt at dealing with the problem of old and sometimes insignificant records. It would appear that the Police are moving towards a general 10 year restriction on access to information concerning minor offences. This will satisfy the requirements of the one time offender who feels that his debt to society has been paid and therefore his record should be forgotten. It will also allow the unusual requirements of a legitimate Police investigation to be considered. The results of this experimentation seem to support the conclusion that certain types of offence data are of minimal relevance to the Police after a period of 10 years without the subject coming under notice.

Proposal (11)

Bearing in mind the present efforts by the Police Department to develop their "culling" experience, the Committee proposes the following:-

- (a) All criminal record data more than 10 years old that comes within the general criteria adopted by the CRO for its "red tick" culling programme, should be regularly culled from active storage. The superintendent-in-charge of the CRO may, if he considers it necessary for Police purposes, or as a matter of public safety, deem that the data should remain in current use.
- (b) (1) Having regard to the experience gained with the restoration of cards from the red tick programme, all data which is culled according to that criteria should be destroyed. This would also apply to the gradual destruction of associated fingerprint and photograph records (where administratively possible). Such destruction would cover almost all offences affected by the provisions of s579.

(2) An alternate proposal to immediate destruction would be the retention of culled data for a period of no longer than 5 years after the original cull. Access to all culled data would require the approval of the superintendent of the CRO on the basis that such access was necessary Police purpose. Such requests for access and approval given should be noted in writing and logged.

- (c) *If an individual considered that his criminal record would come within the culling criteria, he should be able to request that it be culled. To determine whether such culling had already taken place, the individual would merely apply for a copy of his criminal record in the usual way (see Information Bulletin No. 4 July 1976). If this card had been culled, no record would be revealed in response to such a request.*
- (d) *If an individual's request for the culling of his criminal record were refused, reasons should be made available for such a refusal or the applicant should be advised to contact the Privacy Committee if he is not satisfied with the decision.*

5.5 Destruction/Archiving

- 5.5.1 Until 1976 Police had approval from the Archives Authority to destroy the CRO cards and fingerprints of any person born more than 100 years previously. This approval was given in 1964 and again in 1970. In 1976 Police applied to the Authority for permission to destroy records on all those born more than 80 years ago. The Authority refused to grant this, pending a study of the research value of the records revoked its previous approval for destruction and required that all records (CRO and fingerprints) be made available to it for storage as state archives after the 80 year period.

Proposal (12)

The Committee considers that consistent with its proposed recommendation the CRO should have the power to destroy records which correspond to the accepted criteria.

5.6 Recordable and Non-Recordable Criminal Record Information

- 5.6.1 In respect of the offences noted in para. 3.3.7 for which the Police, in their discretion, neither fingerprint nor record on the CRO card, it would appear logical that some universal determination be made as to the recordability of these offences. Rather than have a system where the taking of fingerprints depends on the discretion of the arresting officer, the legislature should declare such minor offences as non-recordable.
- 5.6.2 The subjective system which presently exists is advantageous in that case-by-case decisions are afforded such contemporary information and attitudes as may influence the decisions. However, they suffer from a lack of consistency. Despite the Police circular the final decision still rests with the individual officer and therefore the offender can only rely on the minor nature of the offence and the leniency of the arresting officer. It may afford greater clarity to the present practices if the legislature regularly reviewed offences such as those referred in the Commissioner's directive (see para. 3.3.7) in consultation with the Police and justice administrations in an effort to determine and specify those offences which may not require full fingerprinting and record keeping procedures. This is in no way meant to interfere with the discretion which rests in the Police not to fingerprint. It merely suggests a process of clarification of those offences generally considered not sufficiently serious to require recording. The legislature may also deem fit to independently declare a certain offence "non-recordable" in order to be consistent with current public attitudes or as a preliminary step to decriminalising the offence.

5.6.3 The principal Police objections to the concept of non-recordability are similar to those raised in respect of the expungement of records (see para. 5.2.3). They merit discussion.

- (1) The maintenance of fingerprints and details of arrest and court appearances may be valuable for later police purposes (see para. 5.1.3). However it must be remembered that such non-recordability would mainly be envisaged in situations where the Police currently don't fingerprint anyway.
- (2) Such records should be maintained as a permanent record of petty sessions proceedings. This might be seen as a function of the courts and their record keepers.
- (3) The difficulties of deletion, which would normally arise under the present manual system, could normally be avoided if the non-recordability concept was not made retrospective.
- (4) The criticism of the persistent first offender is only a very minor concern in respect of the conditions under which non-recordability would apply. Where Police already refrain from recording certain offences, they must not see them as serious problems. If the court decides that a 556A dismissal should be non-recordable it makes its own determination that the circumstances of the offence or the character of the offender are such that the court considers it either unlikely that the recipient will offend again or even if he did, the first offence may be of little consequence to any later decision.

5.7 Decriminalised Offences - Deletion or Retention

5.7.1 Where Government policy states that an existing offence should cease to be an offence or, although still remaining an offence should no longer be regarded as "criminal", the problem arises as to old CRO records of offences which are no longer offences or no longer "recordable" offences. Should "decriminalisation" and "non-recordability" be retrospective?

5.7.2 Practicality?

In the existing manual system at CRO it would be very difficult for these offences to be deleted from all existing cards. In any future computerised system, however, there seems no reason why the system could not provide for retrospective deletion of any class of offences, provided that this deletion was anticipated in the early stages of the system. In the existing manual system the only types of deletion possible would be on request, when the record is accessed for any purpose and on any periodic culling of CRO records.

5.7.3 Should Deletion Occur?

The following arguments against removal are basically arguments against any general statutory or administrative rule requiring deletion whenever an offence is repealed. They are not arguments against legislation providing that specific offences which have been repealed should be retrospectively deleted from CRO.

In practice it might often be impracticable to remove these records e.g. if a very broad offence is repealed but is replaced by a narrower offence which still makes illegal some of the conduct previously covered by the broad offence. It might be impossible

to tell solely from CRO records which of the past offences should be deleted. Recourse would have to be had to court records, and the cost could well be prohibitive.

- 5.7.4 Where a previous offence ceases to be an offence, it could be argued that this former offence should no longer be capable of adversely affecting a person and therefore should be removed from CRO.

Arguments for removal:

Although it cannot be argued that a law repealing a crime shows a legislative intent that past conduct constituting that crime should no longer be regarded as having been criminal conduct, this will often be the case in practice.

Arguments against removal:

To do something while it is still illegal is quite different from doing something when it becomes legal. The recording of the offence is not only a recording of the conduct which constituted the offence (which is no longer criminal conduct), but is also a recording of the willingness of the person to break the law and perpetrate such conduct. (The record is therefore still relevant to the person's character and should be recorded). A difficult example is refusal to register for conscription, an offence under the National Service Act.

Proposal (13)

Where an offence has been repealed, limited or specifically replaced by an act of Parliament, it is for Parliament to address itself to the continued maintenance (or destruction) of Police records relating to the original offence.

In general, the Committee would favour the removal of such records from a current, factual and objective store of criminal data such as the CRO.

5.8 Culling or Deletion on Access etc.

- 5.8.1 It has been proposed that the CRO delete the following data:

- (i) arrest details and court appearance details relating to unsuccessful charges (para. 5.2.8);
- (ii) offences falling under s579 (para. 5.3.4);
- (iii) certain offences after a 10 year period.

It has been argued that such deletion or destruction should be carried out automatically when notations relating to (i), (ii) and (iii) are either dismissed or satisfy the time periods laid down for them. Such a deletion programme may prove difficult with the present manual system. It will no doubt become more practical as CRO records are gradually computerised.

- 5.8.2 Three intermediate possibilities for the present system are:

(a) Deletion on Notification:

In the case of unsuccessful charges, all such charge and arrest details should be removed from the cards when the court notifies the CRO of the determination of the charge. At present such notification (i.e. charges dismissed) is usually recorded on the card.

(b) Deletion on Access:

Whenever a CRO card is accessed for any purpose (e.g. an employment or licensing check or preparation of an antecedents report for a court) the details could then be obliterated, the card destroyed if there are no other entries, and any fingerprints/photographs destroyed. As it is already proposed that CRO staff should scrutinise such entries to ensure they are not included in resumes or antecedents reports, it would be possible and practicable for them to delete such entries at the same time. This procedure may be specifically applicable to offences falling under the provisions of s579. Perhaps, at the time of access, all data which satisfies the time requirements of the section should be referred to a senior officer to determine whether deletion should take place (according to the other provisions of s579).

It should be remembered that in N.S.W. the major credit bureaux utilise deletion on access as their main deletion method, although most have an additional culling usually on a periodic basis.

(c) Deletion on microfilming and/or computerisation:

Before a record is microfilmed or placed "on line" it could be inspected and dealt with as with deletion on access. The difference is that access already involves some inspection of the record to see what should be disclosed, whereas microfilming only involves checking that there are no new entries on it for a certain period of time.

Each of the above, when combined with an on going culling programme as suggested in para. 5.4 might provide the most effective rationalisation of records within the limits of a manual system.

CHAPTER 7

Computerisation

7.1 Computerised Records

- 7.1.1 The Police Department is presently undertaking an extensive study to ascertain the most efficient means by which their current manual filing systems will be gradually computerised. The study has not yet been completed, making much of what is said in this chapter both general and tentative. This report relies on the information supplied by the Department in the nature of answers to specific questions, as well as general discussions had between the Committee and Police Officers involved in the computer feasibility study.
- 7.1.2 At the time of writing this report, the Police Department has brought certain areas of its file keeping systems on line as well as having taken specific steps to initiate this transfer in other areas. In order that the present position of the N.S.W. Police Department regarding computerisation might be isolated and examined it is necessary to discuss the following in more detail.
1. Police records presently stored on computer.
 2. Specific proposals for the conversion of other systems to computer storage.

Once these matters have been considered, the privacy issues raised by the computerisation of Police records can be discussed with more certainty.

7.2 Police Records Presently Stored on Computer

- 7.2.1 Following a study carried out by the Research Branch of the Police Department, in 1971, this system was established within the Modus Operandi section (M.O.). The system stores information relating to offences committed, the time and date that the offence occurred, the physical location of the offence, property stolen, the victim's name, information on suspects and any relevant "wanted" information or outstanding warrants which may relate to the crime. Only information relevant to the last two years is kept "on line" and all other information back to the inception of the system is held in storage. (Disc Packs which can be accessed when required.)

This is the only data held by the M.O. section which is presently stored on computer. Conviction and sentence information are not yet computerised and are still manually recorded at the CRO. A manual storage system of M.O. information prior to 1971, and other information not recorded in this system, act as a back up record store. Despite the continual updating of the computer record, certain warrant and wanted information may be out of date, and dismissed charge data may not be recorded. The Police have stated that a proposed review of the system will probably result in the deletion of all suspect/wanted information from this system.

Information for the system is fed into the computer by VDU terminals located in the M.O. section and operated by trained staff. Data stored in the system can be retrieved and displayed on these terminals in a matter of seconds. Police in other divisions or throughout the State can telephone the M.O. section and request and obtain the information they require instantaneously.

An associated benefit in the computerisation of this information is thorough prompt and accurate accessibility for research purposes.

7.2.2 Pistol Licence Review and Stolen Firearms System

Information which relates to the holders of pistol licences and the renewal of such licences is stored on computer, as well as details of stolen firearms, e.g. type, serial number, location, etc. It also contains references to persons refused or prohibited from holding licences under the Firearms or Dangerous Weapons Act, or who had licences revoked or have been convicted of any offences under the Act.

7.2.3 Stolen and Wanted Vehicles System

The Police computer is directly linked to computerised data held by the Department of Motor Transport regarding stolen and wanted vehicles. The link to the DMT computer merely provides the means for checking registration details of a vehicle reported stolen or wanted, to ensure the accuracy of the data accumulated and stored by the Police regarding stolen and wanted vehicles.

7.2.4 Warrants and Wanted Persons Information System

Information as to warrants in this system (known as the Want/Warrants System) has been available on computer since March 1978. Data on wanted persons, as distinct from the warrant system, is computerised only so far as that part of it which is in the CIIS (see para. 2.2). The remainder is in the manual records of the CRO and MO section. All this information on wanted persons is earmarked, for future computerisation after being subjected to a culling and verification process. The records of missing persons and disqualified drivers are the remaining sections of this system to be computerised.

The necessity for rapid response to requests for data on warrants and wanted persons is obvious. Computerisation has overcome many of the delays caused by the use of a manual system in an emergency situation. Another difficulty with the manual system is that notification of executed or cancelled warrants or alleviation of suspicion concerning a wanted person, may not be made on the cards at frequent and regular intervals. The computerised system is intended to protect suspects against errors in information by increasing the efficient updating and removal of information from the system when such information is no longer accurate and relevant, whilst not interfering with rapid access to the data that remains on the system.

All outstanding warrants are periodically fed through the DMT computer in an effort to obtain current address information. This is presently done by submitting written requests and will be later carried out through a direct computer link.

7.2.5 The Stolen Property System

Information relating to serialised stolen property has been brought on line since March 1977. The owner of the property is recorded by reference to the crime report which contains that information. The system is to be extended to include data on property stolen prior to 1977.

7.3 Specific Proposals for Conversion of Other Police Data Systems to Computer Storage

7.3.1 Central Card Index.

The Central Card Index Cards contain the following data:-

1. Personal details of the offender.
2. Details of arrests and their disposition.
3. Details of matters for which the whereabouts of that person is sought (missing persons, warnings for Police regarding the approach of the individual).

7.3.2 All information which is transferred on to the Central Card Index and held in store at the CRO is usually supported by fingerprint identification. The Central Fingerprint Bureau comprises fingerprint forms which contain:

1. fingerprints;
2. personal details similar to those noted on the CCI cards;
3. usually particulars of the arrest and to a lesser extent, the disposition of the charge as noted on the CCI cards.

7.3.3 It is the intention of the Department to computerise the names appearing on all CCI cards, as well as the personal particulars and fingerprint classification details also noted on the said cards. Some indication as to the type of offence for which the subject was recorded may also be included. No projected date for the computerisation of this information is provided by the Department. However, as an intermediate prospect, the normal visual index, which contains this information (e.g. name, age and fingerprint classification) was converted to microfiche in July 1978.

7.3.4 It is also projected that the fingerprint forms presently held in a manual form at the Central Fingerprint Bureau will be computerised in a digital form. Reference will be made at some future date to the subject's record as held in the form proposed in para. 7.3.3.

7.4 Access to Computer Storage

7.4.1 As discussed in ch.4 para. 4.7.3, police records are presently accessed through a "phone in" system. This is also the situation with information presently stored by computer. The only direct terminal access to police computer records is in operation at the central office of the Modus Operandi Division. Any requests for access, external to that Office, are acceded to and the data retrieved through the terminals is conveyed by 'phone to the original applicant.

7.4.2 The Department is presently planning the installation of terminals in certain police stations throughout the metropolitan area with a view to generally extending this system throughout the State. The "phone in" system may still be required to service those stations not in the terminal network. As is presently the case with the manual system, terminal accesses will be logged. However such logging will only identify the terminal, the enquiry (and not the enquirer) and the time and date of the access. On line information will be available to any terminal which satisfies "the right to know" code, devised by the Department's programmers. Thus it is the terminal rather than each individual operator which is intended to demonstrate its bona fides. Some terminals may access one or more parts of one or more systems, whilst others may access all systems. At each station with a terminal, all officers will be empowered to operate the facility. The security of the terminal itself will not be regulated by an operator's code or "key" system, but rather the physical security of the operation will come under the direct supervision of the senior officer in charge of the station.

7.5 Linkages

Police have unrestricted instantaneous access to DMT computer files. The main method presently used is on line enquiry from any of four terminals within the Police Department and thence by telex link to connected police stations. Police terminals are in Foveaux Street (Warrants), CIB (stolen vehicles), Radio Rooms CIB, and the Police Traffic Branch. Information flow would include ownership of vehicles, data on stolen and wanted vehicles, registered addresses of licensees, and traffic offences records. The Committee proposes to discuss the growth of this linkage with the Police. Particularly sensitive are accesses to traffic offences records. The Committee will be formally recommending to the Police that access to DMT traffic offences records be logged according to time and name of enquirer.

7.6 Privacy Concerns in the Computerisation of Criminal Record Data

7.6.1 Increased Scope of Dissemination

The computerisation of criminal records in an on line environment creates incentive for terminal access at both suburban and remote locations. This increase in outside access decreases CRO control over dissemination and uses of records. The decision as to access becomes diffused and local. Also if there is no local control as to terminal use, any person in the station could exercise his own initiative as to access. The problem is particularly acute if the system is designed without a logging facility of all enquiries made. Logging of individual enquirers is the major protection existing in the present manual system.

Dissemination via terminal would also by-pass any personal determinations which are currently made by CRO staff as to the propriety of the access. Whilst the present access system has an in-built discretion in the CRO informant as to whether data should be disseminated, the computer system will automatically divulge it. The only discretion that the computer can exercise is whether the correct code has been input by the requester.

7.6.2 Inflexibility of Design

A more subtle danger may be inadequacy and possibly mis-interpretation of information resulting from the structured nature of storage. Whilst a human can and does make decisions based on broad instructions or policy, a computer can make decisions only on explicit instructions within a prescribed framework as conceived by the limits of human anticipation of the system environment. In the context of criminal record data the cost restraints of computerisation could for instance lead to the exclusion of valuable identifying factors or other vital data. While that data could be squeezed onto a card or communicated orally from special knowledge, it may not be possible to enter it into the less flexible computer. When a policeman needs to know certain information urgently, its inadequacy or incompleteness as a result of the structured nature of computer storage can lead to unfortunate or even of grave consequences. Two examples of this type of danger from the U.S. where computerisation of this type of data exists have been brought to the Committee's attention:

1. A black was arrested on suspicion of car stealing because he fitted the wanted man's description and had the same name; the wanted man was white but the computerised description failed to mention that. The system was designed narrowly and did not include this vital detail.
2. Frank Booth, en route to his father's funeral, was pulled over by a patrolman. The patrolman, advised by radio that the computer recorded the car as stolen, was on edge. Apparently Booth moved the wrong way and was shot dead by the patrolman. The computer had failed to differentiate between a 1971 registration, which had been stolen, and Frank Booth's 1975 registration. If the system had been designed to anticipate this type of problem, the computer could in fact protect privacy. Unfortunately, however, a systems designer cannot anticipate every possible beneficial use within the system environment. Meanwhile, the greater reliance a person puts on the efficiency of the system, the greater faith that person has in its absolute accuracy. This can lead to complacency. See 7.6.3 below. In this case the policeman failed to evaluate the worth of the data by distinguishing the registration dates from the year model of the car. He simply relied on his faith in the magic of structured data without applying his mind to the actual circumstances.

7.6.3 Human Complacency

The more dependent man becomes on computers, the greater will be the tendency to believe in the system's utter infallibility. Information flashed onto a screen, symmetrically and with such a mechanical authority, leaves little scope for questioning. The attitude that develops is that it must be correct. Complacency sets in. The analogy can be drawn with the situation where one is more likely to question or change a written draft than a typed copy. In the computer age, the ostensibly always accurate screen picture will usurp the typed copy of the criminal record (with its more obvious manifestations of human error). The myth of the computer, its precise lay-out and reputation as an error-editor, cannot disguise its essential weakness: "garbage in, garbage out". Unfortunately, the recipient of computerised data is generally too mystified by the perfect format to be questioning of the content.

7.6.4 Centralisation and Growth of Records

Computers facilitate the storage of large volumes of data very cheaply. Also the cost effectiveness of large scale computers with cheaper per unit processing power is a good incentive for centralisation. The computerisation of N.S.W. criminal records today could be the first step to a centralised interconnected system of all police records throughout Australia. Also, as storage becomes cheaper, the tendency may be to record a greater amount of subjective or intelligence type information on the central store. The implications of this potential for centralisation and growth of records, compound the privacy problem.

This abundance of information may also impede the efficiency of the current record dissemination system in that the enquirer may receive far more information from the computer than is necessary for his original request. Such problems may arise from an inability on the part of the person requesting the data to stipulate the limits of his information requirements, or he may be prompted to enquire for further details from the computer.

- 7.6.5 At this stage the Committee does not intend to raise detailed proposals relating specifically to computerised police records. It does however consider that a detailed assessment should be

made as to the effective security value of a comprehensive logging system when compared with the costs involved in introducing such safeguards. Both the CRO and the Committee are concerned with the problem of unauthorised access and believe that the best possible security protections should be incorporated into any alternate storage systems.

- 7.6.6 The Committee does, however, consider that the culling/destruction proposals referred to in para. 5.4.3 should be directly applicable to a computerised system of data storage. Culling should take place on the basis of the criteria discussed at the time that the data is being prepared for computer storage.

The Committee further proposes that the system itself be designed as flexibly as possible, but with built-in privacy protections, so that both efficiency and privacy can be simultaneously achieved. It is specifically proposed that (1) each entry for access be logged according to the number code of the policeman making the enquiry; and (2) offences also be coded to assist any future extractions, culling, or destruction. Consideration should also be given to possible linkages with other systems with a view to reduction of data no longer necessary for police purposes. (For example, the matching of the CRO file with a deaths file from the Registry of Births, Deaths, and Marriages could be one method of culling from on-line to micro-storage.)

- 7.6.7 It is accepted that computerisation allows for a greater flexibility both in the introduction and removal of data from storage. With a development of experience in the types of information necessary as a reference for modern police procedures, there should exist a corresponding awareness of the computer's facility to correct, update and refine the data it stores.

CHAPTER 8: JUVENILE SHOPLIFTERS' INDEX

8.1 History

- 8.1.1 Although not a criminal record in the strict sense of the term, the Shoplifters' Index provides an example of an attempt to achieve some form of intermediate reference of a criminal occurrence, without creating a permanent criminal record. This approach takes on particular significance when one realises it is specifically related to juveniles. The Committee does not necessarily in any way endorse the collection and storage of such data on suspected adult shoplifters.
- 8.1.2 The system was developed between the Retail Traders Association and the Police Department and commenced in 1966. While wishing to safeguard the future prospects of the child as far as possible, there appeared to be little deterrent value in simply reprimanding the child and letting him go. However, this reporting scheme emerged as a viable alternative.
- 8.1.3 In view of the lack of precision with which the scheme was introduced, and the passage of time since its inception the procedure has come to vary from store to store. At present it needs to be clarified and made uniform. It will still be left to each individual store to determine whether or not it prosecutes in a particular instance.
Proposal (14)

Firms that are to participate in the index shall be nominated by the Retail Traders Association for approval by the Commissioner of Police and only designated security officers have access.

8.2 Present Procedures

- 8.2.1 All persons under the age of 18 years, detected and apprehended for shoplifting in stores which are a party to the system, will be questioned as to the circumstances of the alleged offence and details recorded on the special reporting forms. (Annexure 8)
- 8.2.2 The reports are in duplicate, are numbered in sequence and are signed by the child.
- 8.2.3 When the identity of an alleged offender is established, the Juvenile Records Section (JRS) of the Police Department is contacted by 'phone to check whether the detainee is known to the Police through the Index.
- 8.2.4 The store usually tries to contact the parents of the child. While practices vary it is usual to ask the child to have one of his parents contact the store. If this does not occur, a letter in the form of Annexure 9 is sent to the parent. The parent does not usually sign the report.
- 8.2.5 If the detainee is previously recorded in the Index (para. 8.2.3) then after discussion with the parent he may be given into the charge of the Police for further action. If he was not recorded, then the store would most likely not proceed but a card would be opened in the Index of the occurrence.
- 8.2.6 Particulars of the action taken in either case are included in the report, stating the names of the Police Officers in the Station if the Police are involved. Otherwise, a notation such as "released to parent" should be included. This is then forwarded to the JRO and a card opened.

- 8.2.7 It would appear that all enquiries made to the Police are channelled centrally through each retail organisation and the name of the person responsible for making the contact notified to the Police. Every such telephone check made to the Police must be confirmed by a report in writing to the Police.
- 8.2.8 Originally, when the index was opened, approximately six people were authorised suppliers of information. This has grown to over sixty and there is little control over the persons from whom information is received. Approximately ~~20,000~~ 3,000 reports are received each year but only about 300 enquiries answered. This shows that stores are rarely checking the index. This may be due to the security officer's aversion to involving the Police and being required to appear in court, and may reveal a preference for using the system as a deterrent to future shoplifting. It is impossible to say whether or not this is effective but it should not be readily discounted.

Proposal (15)

Stores should not exchange information on juvenile shoplifters but rather should rely on the index as a reference for such individuals.

- 8.2.9 The Retail Traders Association states specifically that this reporting scheme is not to be used by their members in connection with any employment decisions. The honesty of an applicant for employment is not to be ascertained by reference to the Shoplifters' Index. The index is however accessed by the Police Department in respect of applicants for entry to the Police Force.

Proposal (16)

Due to the fact that the data held on the index is not a record of the subject's proven involvement in a criminal activity nor have the alleged facts been considered by a court for its determination, the Police should discontinue access for employment purposes. (This is consistent with the Committee's approach to unsuccessful charge details, see para. 5.2.8 .)

- 8.2.10 While the cards are merely identified in the JRO by being of different colour, they are not used for reporting for any other purpose such as sentencing, applicants for employment in the Public Service, etc.

Proposal (17)

That the index be kept separately from all other juvenile record data.

- 8.2.11 The copy of the report is retained by the store for varying periods but usually approximately 12 months.

Proposal (18)

Stores should destroy duplicate report forms within 12 months.

The cards are culled by the JRO approximately after the 20th birthday of the child depending on how regularly the cull is conducted. They are then placed on microfilm.

Proposal (19)

All shoplifting index cards be destroyed within six months of 18th birthday. Such culling and destruction shall occur both at time of access and as a part of a regular culling procedure for the index.

8.3 Problems with the Shoplifters' Index

8.3.1 Despite the Committee's support for a system which introduced some flexibility into the treatment of juvenile offenders, there are some aspects of the system which raise matters for concern.

- (a) The child signing the report: The practice of having the juvenile detainee sign the statement of brief details of the offence seems to be both unnecessary and improper. The Committee considers that one of the most important features of the system is the encouragement of parental involvement. It would be impractical for the Security Officers in a store to require the presence of a parent before taking details from the child. This may often cause the erring child to be detained in a distressing situation for a considerable time, especially where both parents are working or are unable to arrive on the scene post haste. If, however, the child's parent is not to be present we would consider it to be against the spirit of recent amendments to the Child Welfare Act, 1939 (no. 20 of 1977) to require the child to sign any statement.(1)

The Committee is of the view that rather than the child signing the statement of details, every effort should be made to have the parents contact the store and sign the form.

There should, however, be a discretion with the security officer not to inform the parent if the officer considers the child's physical or emotional safety would be gravely at risk if such information were given. If this discretion is exercised it should be fully noted on the report.

Proposal (20)

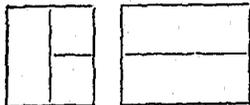
That the parent, not the child, should sign the report form or there be an endorsement as to why the parent's signature could not be obtained.

- (b) At present the child is usually given a letter for his parents requesting that they "call the store urgently during trading hours to discuss something which happened while the child was in the store". The benefit of this parental involvement is not only that it reinforces the seriousness of the situation to the child and provides an opportunity for the parents to be fully informed of the facts but it also acts as a check on the identity of the child detained. Due to the fact that no fingerprints are taken, other assurance that the juvenile has correctly identified himself may be given by the parents. The Committee is in full agreement with the present letters and the fact that they are given to the children to deliver of their own volition. It is also necessary that further contact be attempted if the parents do not reply.

-
- (1) The amendment requires the Police interviewing a juvenile at a Police Station to contact the parents before any statement is taken from the young person involved.

APPENDIX 1

N.S.W. POLICE



F.P.C. _____

P. 59 MALE

ST 726

| | |
|---|--|
| <p>Surname _____ (Block Letters)</p> <p>Christian names in full _____ (Block Letters)</p> <p>Date of birth _____</p> <p>Station where prints taken _____</p> <p>Date prints taken _____</p> <p>Signature of member of the force taking prints _____ (Block Letters below signature)</p> <p>Rank _____</p> | <p>RIGHT FINGERS</p> <p>Initials of Station Sergeant _____</p> |
|---|--|

| 1. Right thumb | 2. Right index-finger | 3. Right middle-finger | 4. Right ring-finger | 5. Right little-finger |
|----------------|-----------------------|------------------------|----------------------|------------------------|
| | | | | |

This form must be completed in every detail before the Officer concerned begins to take the fingerprints of any other person.

| | | | |
|---------------------|-------------------------------|---|-------------------------|
| <p>LEFT FINGERS</p> | <p>Index Checked by _____</p> | <p>Classified and Searched by _____</p> | <p>Checked by _____</p> |
|---------------------|-------------------------------|---|-------------------------|

| 10. Left little-finger | 9. Left ring-finger | 8. Left middle-finger | 7. Left index-finger | 6. Left thumb |
|------------------------|---------------------|-----------------------|----------------------|---------------|
| | | | | |

LEFT INTERDIGITAL:

RIGHT INTERDIGITAL:

ALL PARTICULARS TO BE TYPED OR PRINTED

Name in full (with alias)

(Block Letters)

Date of Birth _____ Age _____

(Day, Month, and Year)

Birthplace, Town
and Country _____

Arrival in
Australia { Date _____
Slip _____

Height _____ mm Build _____

Complexion _____ Hair _____ Eyes _____

Occupation _____

Address
in full _____

Court Sentenced
or remanded at _____

Date _____

Offence
in full _____

Sentence or date
remanded to _____

Arrested by _____

Descriptive marks, including scars, tattoo marks, physical deformities and other peculiarities, etc.

If known, names of persons with whom arrested:

When a finger is missing, or so injured that the impression cannot be obtained or is deformed, and yields a bad print, the particulars and the date of loss of finger or injury must be stated.

THE FOLLOWING PARTICULARS MUST BE WRITTEN BY THE PERSON WHOSE FINGERPRINTS ARE TAKEN

THUMB PRINTS TO BE TAKEN (Rolled)
Right Thumb Print Left Thumb Print
(To be impressed immediately after signature, etc. is written)

Date of birth _____ Age _____
(Day, Month, and Year)

Signature _____

Address
in full _____



SAMPLE COPY.

(P. 2200)

RE:

Brian WILLIAMS

Conviction Records Section,
Criminal Records Office,
Criminal Investigation Branch,
SYDNEY

33/33 W/W IMO/OCO 44/26 F.P.C.

10-10-50 D.O.B.

Nil Photo Ref.

The fingerprints of the abovementioned person who was charged at

Darlinghurst on the

10-10-76

for the offence/s of

Stealing

are identical with those of

Brian Thomas WILLIAMS ;

who has been before Court *as follows/*as per attached list.

| COURT | DATE | OFFENCE | RESULT |
|------------------------|---------|---------|--------|
| Last appeared Brisbane | | | |
| | 30 9 76 | | |
| and five other | | | |
| entries... | | | |

* Strike out whichever is not applicable.

St 443

THE POLICE PROSECUTOR

CENTRAL

11-10-76

JRA

Where a person is charged with stealing or larceny, the nature of the property stolen, the Act and section under which the charge was laid, the NAMES OF ANY PERSONS CHARGED WITH OFFENDER AND THE RESULT OF THE PRESENT CHARGE/S, SHOULD BE SUPPLIED OVERLEAF.

For SUPERINTENDENT IN CHARGE

APPENDIX 2

| No. | Court | Date | Offence | Sentence | Police Gazette Reference |
|-----|-------------------------------|---------|--|--|--------------------------|
| 1 | N.S.W. Lithgow F.S. JF. | 6.6.72. | Embezzlement. | Committed for sentence Penrith C.S. 1.8.72. | |
| 2 | Penrith Q.S. | 11.8.72 | Embezzlement | Bound over to be GB 2 appear for sentence if called w/in 3 years; further conditioned that he pay \$650 compensation & submit to supervision & guidance of Adult Probation Service. | 72/185 |
| | | | HISTORY FC (11.5.6.75m | | |
| 3. | QUEENSLAND Brisbane M.C. | 23.5.75 | Stealing & charges Possession of property. | Admitted to Probation for 2 years restr. \$183 within 9 months. on all charges. | |

| No. | COURT | DATE | OFFENCE | SENTENCE | P. Gazette Reference |
|-----|---------------------|----------|---|--|----------------------|
| 4. | Nambour M.C. kfw | 29.9.75 | Stealing | Fined \$30 In default 7 days imp. | |
| 5 | Brisbane M.C. rl | 14.11.75 | Stealing (8 charges) Possess property suspected stolen. | 3 months on each charge 3 months imp. | |
| 6. | Brisbane M.C. lj | 30.0.76 | False pretences. | 3 months imp. | |

1. SMITH
 SURNAME

John
 Christian Names

P. 59D

See Card 2

St 2766-2

Birthplace Sydney N.S.W.
 Date of Birth 16-9-32
 Arrival in Australia } Date _____ Ship _____
 Height 180 cms Ft. _____ Ins. _____
 Build Medium
 Complexion Fair
 Hair Brown
 Eyes Blue
 Occupation Saleman
 Other Marks and Peculiarities
Swallow on right upper
arm. Death before dishonor on left
upper arm.

SAMPLE CARD ONLY.

Fingerprint Classification
 1 R 233 19
 1 R 654 21

Docket Number

If in Single

DATE Card made and
 by whom

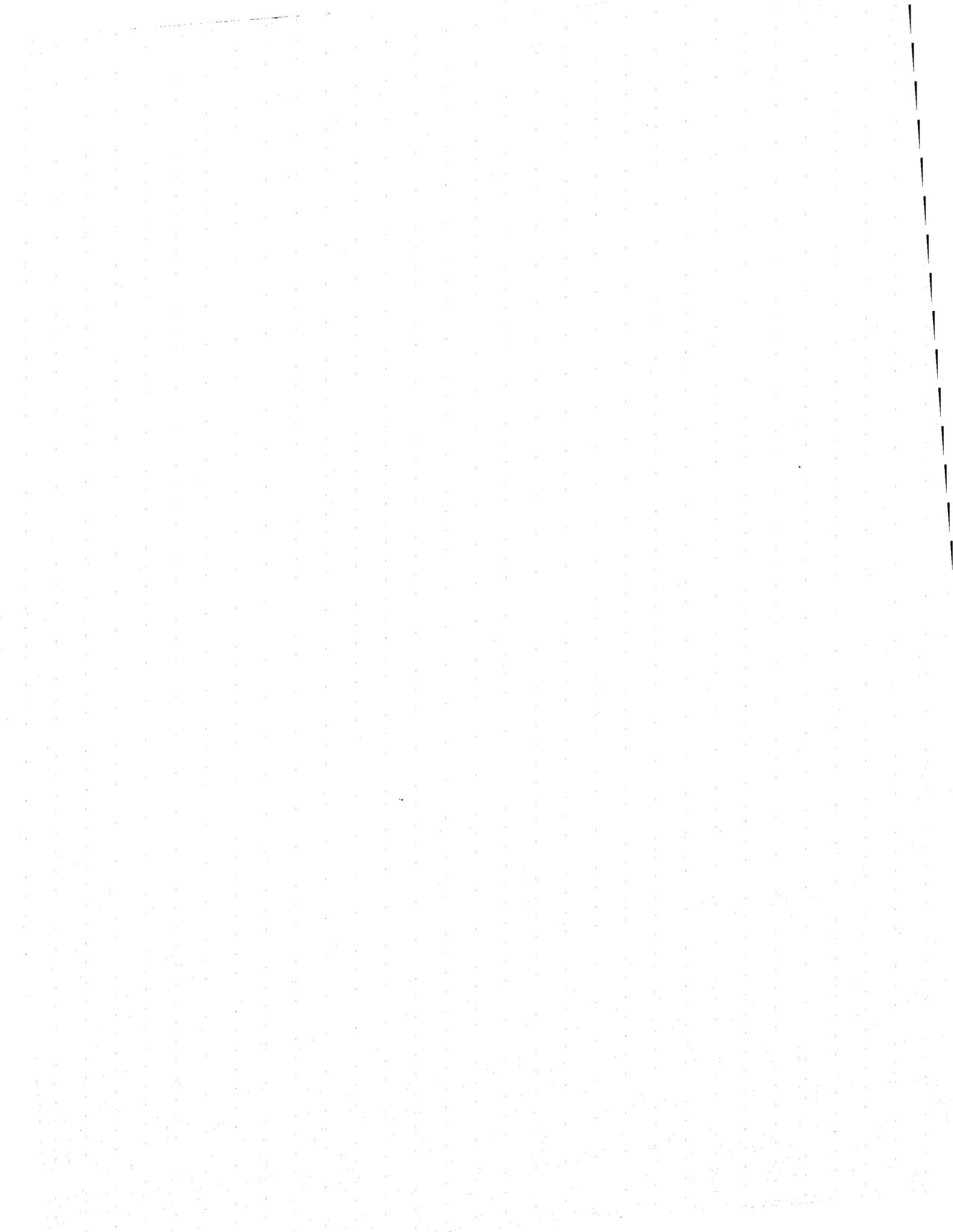
13-10-76 JRA.

671206

| No. | Name and Address | Date of Arrest | Arrested by | Station Charged | Gaol Discharged from and Date | With whom Arrested C. B. Information |
|-----|--|----------------|-------------------------|-----------------|-------------------------------|--------------------------------------|
| 1. | John SMITH 1/29 King Street, Coogee. | 12-10-76 | Const. Quinn | DARLINGHURST | | |
| 2. | John William SMITH. 1/29 King Street, Coogee. | 14-10-76 | Sen. Const. Anderson | MARQUESS | | |
| 3. | John William SMITH 1/29 King Street, Coogee. | 17-10-76 | Sgt. 3/C Grant | WAVERLEY | | |

| | | | |
|------------|---------|--|-----------------------|
| SMITH John | 16-9-32 | | 1/1 R/R 233/654 19/21 |
| | | | |

| | | | |
|--------------------|---------|------------|-----------------------|
| SMITH John William | 16-9-32 | SMITH John | 1/1 R/R 233/654 19/21 |
| | | | |



| | | | |
|------------------|--|----------------------|--|
| SIRNAME | | SPECIAL PHOTO NUMBER | |
| CHRISTIAN NAMES | | | |
| DATE TAKEN | | WHERE TAKEN | |
| OFFENCE | | | |
| RECORD NAME | | | |
| POLICE IN CHARGE | | RIGHT INDEX PRINT | |
| WHERE STATIONED | | | |
| PHOTOGRAPHER | | | |
| F.P.C. | | | |
| M 2721 | | | |

OFFENDER IDENTIFIED BY _____
RANK _____

| DESCRIPTION | | |
|------------------------|--------|---------|
| DATE OF BIRTH | EYES | |
| PLACE OF BIRTH | | |
| OCCUPATION | | |
| COMPLEXION | BUILD | |
| HAIR | HEIGHT | FT. INS |
| IDENTIFYING MARKS ETC. | | |
| | | |
| | | |

APPENDIX 6

CORRECT NAME:
ALIASES:
ADDRESS:

P. 245

SEX:
DATE OF BIRTH:

M. 1483 V. C. N. Blight, Government Printer

| Offence and date | Station and File No. | Committed in Company with | Adjudication and date | Cautioned or Court decision and date | Conduct during six months |
|------------------|----------------------|---------------------------|-----------------------|--------------------------------------|---------------------------|
| | | | | | |

SHOPLIFTING OFFENCES BY JUVENILES

P.245A

Name:
Address:
School attended or/
Place of Employment:

Sex:
Date of Birth:
Marks, physical defects, etc.:

| Name and Address of Store | Date detected | By whom detected | Brief particulars of offence |
|---------------------------|---------------|------------------|------------------------------|
| | | | |

DATE
& TIME

POLICE

PERSONS INQUIRED FOR

REASON

RESULT

| DATE & TIME | POLICE | PERSONS INQUIRED FOR | REASON | RESULT |
|----------------|---|--|------------------------------------|------------------------|
| | Name <i>Sgt. Nicolson</i> Rank <i>Sydney</i> Station <i>10th Division</i> Reg. No. <i>3527</i> | <i>John Thomas Buchanan</i> <i>2 1 36</i> | <i>Receipt</i> <i>not found</i> | <i>Yes</i> <i>✓</i> |
| | Name Rank Station Reg. No. | | | |

Date

Report No.

SHOPLIFTING OFFENCES BY JUVENILES

Name of Store:

Address:

NOTE: Details on this form are to be typed in and the original forwarded to the police. The duplicate is to be retained in safe custody.

CHILD

Surname
Christian Names
Address
Date of Birth
School attended or
place of employment

PARENTS

Father

Name
Address
Occupation

Mother

Name
Address
Occupation

APPREHENDED

Name
Phone No.

BY

Brief Details of Offence:

Signature of Witness:

Signature of Juvenile:

APPENDIX 9.

.....
.....
.....

Dear Sir/Madam,

A child who identified himself/herself as
and named you as parent or guardian, visited our store on
.....

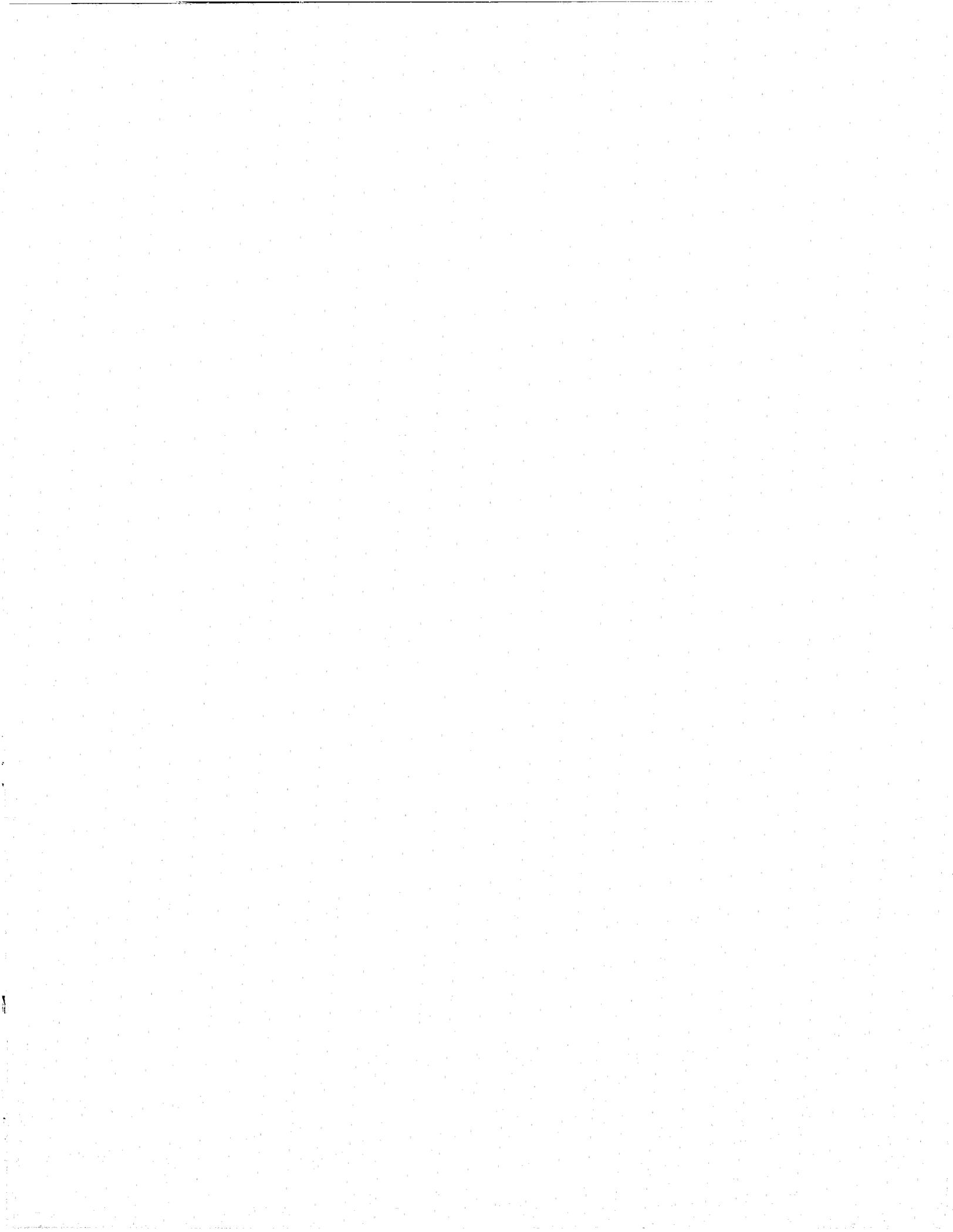
We are most anxious to discuss with you something which happened while the child was in the store.

Would you please call at the store urgently, during trading hours, and ask for my office. There is no need to make an appointment but it would be of help if you could bring the child with you.

If you cannot call, please 'phone me (telephone no.
extension) within the next two days so that we can make an alternative arrangement.

Yours faithfully,
for GRACE BROS. PTY. LIMITED.

Senior Security Officer.



END