



**PROTECTING
CONFIDENTIAL
INFORMATION**

**A REPORT ON THE IMPROPER ACCESS TO,
AND RELEASE OF,
CONFIDENTIAL INFORMATION FROM THE POLICE
COMPUTER SYSTEMS BY MEMBERS OF THE
QUEENSLAND POLICE SERVICE**

NOVEMBER 2000



CJC Mission:

To promote integrity in the Queensland Public Sector
and an effective, fair and accessible criminal justice system.

© Criminal Justice Commission 2000

Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the **Copyright Act 1968**, no part may be reproduced by any process without permission. Inquiries should be made to the publisher, the Criminal Justice Commission.

ISBN 0 7242 7163 5

Criminal Justice Commission, 140 Creek Street, Brisbane, Australia 4000
PO Box 137, Brisbane Albert Street Qld 4002
Tel.: (07) 3360 6060, Fax: (07) 3360 6333, Email: mailbox@cjcc.qld.gov.au
Web site: www.cjcc.qld.gov.au

**Note: This publication is accessible through the CJC home page —
www.cjcc.qld.gov.au — for a limited period.**



The Honourable Peter Beattie MP
Premier of Queensland
Parliament House
George Street
BRISBANE QLD 4000

The Honourable Ray Hollis MP
Speaker of the Legislative Assembly
Parliament House
George Street
BRISBANE QLD 4000

Mr Paul Lucas MP
Chairman
Parliamentary Criminal Justice Committee
Parliament House
George Street
BRISBANE QLD 4000

Level 3 Terrica Place
140 Creek Street
(Crm Adelaide & Creek)
Brisbane Qld 4000

PO Box 137
Albert Street
Brisbane Qld 4002

Telephone
(07) 3360 6060

Facsimile
(07) 3360 6333

Toll Free
1800 06 1611

Email
mailbox@cj.cqld.gov.au

Dear Sirs

In accordance with section 26 of the *Criminal Justice Act 1989*, the Commission hereby furnishes to each of you its report *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service*. The Commission has adopted the report.

Yours sincerely

A handwritten signature in black ink, appearing to read "Brendan Butler".

Brendan Butler SC
Chairperson

FOREWORD

This report presents the results of a review, undertaken by the Criminal Justice Commission (CJC), of the information-security policies, procedures and practices of the Queensland Police Service (QPS). The report puts forward a comprehensive set of recommendations, which, if implemented, should substantially reduce the risk of police officers and other QPS employees improperly accessing and releasing confidential information held in the police computer systems.

The review was prompted by a CJC investigation, initiated in August 1998, into allegations that police officers stationed at the Nerang Police Station may have been unlawfully disclosing confidential government information from the QPS computer systems to a cleaner who was employed at that station. Initial investigations suggested that the allegations had substance and that the suspected misconduct was widespread.

During the course of the investigation, the CJC received other allegations of police officers unlawfully disseminating QPS information. In addition, there was a steady flow of similar complaints that could not be productively investigated because of issues relating to current QPS information systems. In order to investigate those matters that the CJC could pursue, it was decided to commence an inquiry known as Project Piper.

In December 1999 the Commission resolved to conduct hearings into the alleged improper access to, and release of, confidential information from the police computer systems by members of the QPS. At the conclusion of this investigative phase of the Inquiry, the CJC heard submissions from interested stakeholders over three days of public discussion in order to ensure that all issues were considered from a number of perspectives.

The evidence that the hearings and the submissions disclosed led the CJC to take a proactive approach aimed at reducing the future incidence of improper access to, and/or release of, confidential information. This process was undertaken with the support of the Commissioner of Police, who acknowledged the challenges posed by technological developments in recent years. On this, as for other issues, the CJC has sought to work with the QPS in the shared objective of continuing the reform process.

The report has required a balancing of many difficult and important issues and concerns. However, we are satisfied that the recommendations made in it are workable, while providing for a proper level of accountability. As is standard practice, there has been extensive consultation with the QPS in the finalisation of the report.

Although the report draws attention to deficiencies in the QPS systems for managing information security, it should be recognised that major gains have been made by the QPS over the last decade in raising levels of integrity within the Service and reducing the opportunities for misconduct. With respect to the specific area of information security, the QPS has developed an information-security policy-development framework that has resulted in comprehensive policies and procedures to reduce the risk of breaches of information security. The Service has also developed a comprehensive computerised information system that includes a facility to examine any transactions conducted by computer users. More generally, significant steps have been taken to build up an 'integrity framework' within the Service as a whole, as evidenced by such initiatives as the establishment of the Ethical Standards Command. The recommendations made in this report represent a collection of complementary changes and initiatives that will further reduce the risk of misconduct within the Service.

It should be acknowledged that the problems that have been identified in relation to

QPS systems and processes are not unique to the QPS but, rather, are characteristic of large police organisations in general, and most likely of many other non-policing bodies. However, the fact that the problems are not restricted to the QPS is not, of course, a justification for inaction or delay in addressing these problems.

The report is primarily concerned with the QPS but it will be of interest to all areas of government because a wider range of information is increasingly available to public-sector employees. It is important that agencies and departments take a strategic and proactive stance in the development of information-security systems. To do otherwise may result in embarrassing and costly breaches of information security.

As is standard practice for inquiries of this nature, the CJC will monitor the implementation of recommendations made in this report and may make a further report to Parliament, if this is considered necessary.

Brendan Butler SC
Chairperson
Criminal Justice Commission

ACKNOWLEDGMENTS

This report reflects the contribution and work of many individuals. The analysis of the material relating to the Nerang Police Station, in particular, was painstaking work and involved many months of ‘hard slog’ by investigators. The members of the investigative team are to be commended on their efforts — Detective Superintendent Ann Lewis, Acting Executive Legal Officer Peter Lyons, Detective Inspector Neil Armstrong, Detective Sergeants Sandy Brightwell and Steve Whitelaw, Civilian Investigators Rod Paddon-Jones and Graham (Mick) McMullen, Intelligence Officers Michelle Chapman and Amos Mackay and Financial Analyst Gina Look. The team also made a valuable contribution to the development of the recommendations contained in the report.

Together with Mr Darryl Harvey, Gina Look and Linda Waugh also played a significant role in preparing and presenting electronic evidence at the public hearing. This was the first time that the CJC had used electronic evidence in this way and its success has guaranteed that it will be used more in the future.

The CJC was greatly assisted by Mr Ralph Devlin of Counsel, both in terms of the efficient running of the hearings and through his sound tactical and legal advice.

The CJC is also grateful for the contribution of two officers from the Ethical Standards Command of the Queensland Police Service, Detective Inspectors Robert Holland and John Maloney. Both assisted in CJC investigations, especially those concerning the officer at the Inala Police Station. Particular thanks must also go to the Manager of the Information Security Section, Ms Carolyn Allinson, Senior Sergeant David Crane and other staff of the Section who provided extensive assistance during the investigation and at the public hearing.

At the conclusion of the investigative phase of the Inquiry, the CJC heard submissions from interested stakeholders over three days of public discussion. The goal was to gather information from a range of sources to ensure that all issues of importance were considered from a number of perspectives. The CJC is grateful for the contributions of stakeholders, through their written and oral submissions. These were of enormous assistance in the development of comprehensive and workable recommendations.

Mr Forbes Smith (Deputy Director, Investigations) and Ms Linda Waugh (Senior Research Officer, Research and Prevention Division) had primary responsibility for drafting this report and the recommendations made herein.

Ms Maggie Fitzhenry provided invaluable support through the entire project; her efforts are greatly appreciated. Ms Tracey Stenzel provided support and advice in the preparation and presentation of the final report. Other staff, including Ms Margot Legosz, Ms Terri McTegg, Ms Lisa Evans and Ms Sue Peachey, are also thanked for their invaluable contributions in producing this report.

The report was edited by Cunnington Publishing, desktopped by Rene Graphics and printed by Goprint.

CONTENTS

Glossary	xii
Executive summary	xvii
List of recommendations	xxiv
Chapter 1: Introduction	1
Scope of report	1
CJC jurisdiction	2
Genesis of investigation and background to Inquiry	4
Structure of the report	6
Conclusion	6
Chapter 2: The central issues	7
What is information security?	7
The market for information and the brokers who facilitate information exchange	11
Legislation to protect information	11
Conclusion	14
Chapter 3: The investigation	15
Nerang Police Station	15
Inala Police Station	20
Fortitude Valley Police Station	21
North Queensland Police Station	22
Southport Police Station	23
Conclusion	25
Chapter 4: The nature of the misconduct	27
Previous CJC experience	27
The difficulties frustrating productive investigation	28
The motivation to commit this type of misconduct	29
Complaints statistics as an indicator of prevalence	29
The potential for abuse	31
The marketability and value of confidential information	32
Stakeholder concern for the protection of information	36
QPS submission on funding	37
Conclusion	39
Chapter 5: Information security in the QPS	41
Information security and the responsible organisational units	41
The organisational response to information security	43
Release of information and accessing the QPS computer systems	45
Conflicts of interest	47
Disposal of information printed from computer systems	47
The technology of information security	48
Use of audit-trail information	48
Training and education in computer use and information security	49
Information-security awareness and individual accountability	50
Conclusion	50

Chapter 6: Improving information security in the QPS	53
Method of analysis	54
An organisational response to information security	54
The location of the Information Security Section	56
Corporate/mainframe computer access for authorised users	56
Corporate/mainframe computer access using another person's user-ID	58
Conflicts of interest	60
Disposal of information printed from corporate/mainframe computer systems	61
The technology of information security	62
Systematic and ongoing internal audit	64
'Reason for transaction' requirement	66
Information-security awareness and individual accountability	72
Training and education in information security	75
Conclusion	76
Chapter 7: The market for information	77
Observations made during this Inquiry	77
Current systems and provisions for accessing government information	80
Why are private investigators being employed to obtain illicit information?	87
Conclusion	90
Chapter 8: Industry regulation in Queensland	91
The concern about the industries	91
Commercial agents	92
Private investigators	96
Non-government associations and institutes	98
CJC comment on industry regulation	98
Conclusion	104
Chapter 9: Information protection and the law	105
Unlawful access to confidential government-held information by members of the QPS	105
Unlawful release of confidential and/or personal information	106
Unlawfully obtaining confidential personal information	107
The issue of privacy	108
Conclusion	109
Chapter 10: Keeping the issues on the agenda	111
Final comments on the three central issues	111
The lessons for all government departments and agencies	113
Implementation of recommendations	113
Endnotes	115
Appendixes	117
Appendix A: Examples of in-confidence material	117
Appendix B: The ICAC experience in relation to conducting public hearings	118
Appendix C: Legal advice on conducting public hearing	120
Appendix D: Announcement of CJC Inquiry	122
Appendix E: Guidelines used to make non-publication orders during the public hearing	123
Appendix F: List of stakeholders who made submissions to the Inquiry	124
Appendix G: Information privacy principles (Australian Commonwealth)	126
Appendix H: Excerpt from the Queensland Government Information Standard 24 (Privacy and Confidentiality)	130
Appendix I: The QPS SELF Test	131

Appendix J: Structure of the Information Security Section, QPS	132
Appendix K: Structure and reporting relationships of the Information Management Division, QPS	133
Appendix L: Structure and reporting relationships of the Ethical Standards Command, QPS	134
Appendix M: QPS assessment criteria for outside employment	135
Appendix N: Warning screen that appears when logging into POLARIS	136
Appendix O: Warning screen that appears when logging into the QPS System	137
Appendix P: Excerpt from Police and Drugs: A Follow-up Report (1999a)	138
Appendix Q: Documents and reports available from TIRS and CRISP	140
Appendix R: Reason for Transaction field in the TIRS and CRISP systems	142
Appendix S: CITEC CONFIRM fees for searches on vehicle registrations, TIRS and CRISP databases	143
Appendix T: Sections 67 and 68 of the Transport Operations (Road Use Management Vehicle Registration) Regulation 1999	144
Appendix U: Excerpt from ICAC Report on the Unauthorised Release of Government Information (1992)	146
Appendix V: Schedule of offences under the Criminal Code excluding applicants from obtaining a private investigator licence	149
Appendix W: Meaning of penalty unit under the Penalties and Sentences Act 1992	150

References	151
Further Reading	153

GLOSSARY

Abbreviations:

ACID	Australian Criminal Intelligence Database
Act (the)	Criminal Justice Act 1989
CAP	Competency Acquisition Program
CJC	Criminal Justice Commission
CRISP	Crime Reporting Information System for Police
DVO	Domestic Violence Order
ESC	Ethical Standards Command of the QPS
FYC	First Year Constable
HRMM	Human Resource Management Manual of the QPS
ICAC	Independent Commission Against Corruption (New South Wales)
IMA	Institute of Mercantile Agents
IMD	Information Management Division of the QPS
IPPs	Information privacy principles
ISC	Information Steering Committee
ISS	Information Security Section of the QPS
IT	Information Technology
LCARC	Legal, Constitutional and Administrative Review Committee
LEAP	Law Enforcement Assistance Program (used by Victoria Police)
NEPI	National Exchange of Police Information (now known as CrimTrac)
NPRU	National Police Research Unit (now known as the Australasian Centre for Policing Research)
NSW	New South Wales
OECD	Organisation for Economic Co-operation and Development
OMD	Official Misconduct Division of the CJC
OPM	Operational Procedure Manual for the QPS
PIC	Police Information Centre (QPS)
POCC	Police Operational Conversion Course (QPS)
PROVE	Police Recruit Operational Vocational Education (QPS)
PSAA	Police Service Administration Act 1990
QMVR	Queensland Motor Vehicle Registration
QPS	Queensland Police Service
SAPOL	South Australia Police Service
TIN	Traffic Incident Number
TIRS	Traffic Incident Recording System (owned by the QPS)
TRAILS	Transport Registration and Integrated Licensing System (owned by Queensland Transport)
VICPOL	Victoria Police

Technical terms and definitions:

Access	Opportunity to make use of an information system resource.
Access control	Limiting access to information-system resources to authorised users, programs, processes, or other systems only.
Accountability	Principle that responsibility for ownership and/or overseeing of information-system resources is explicitly assigned and that assignees are answerable to proper authorities for stewardship of resources under their control.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established security policies and procedures, and/or to recommend necessary changes in controls, policies or procedures to meet security objectives.
Audit trail	Chronological record of system activities or message-routing that permits reconstruction and examination of a sequence of events.
Authorisation	Access privileges granted to a user, program, or process.
Biometrics	Automated methods of authenticating or verifying a user by means of physical or behavioural characteristics.
Charge record	Allegations recorded against a person. In accordance with the Criminal Law (Rehabilitation of Offenders) Act 1986 , a charge is an allegation formally made in court that a person has committed an offence where: (a) the allegation is not pursued to a final determination in a court; or (b) a conviction is not recorded by a court in respect of the allegations; or (c) a conviction recorded by a court in respect of the allegation is deemed, pursuant to law, not to be a conviction.
Command query	The action of interrogating some QPS computerised information systems (e.g. conducting a search of driver's licence by name).
Commercial agent	Definition as it appears in the draft Property Agents and Motor Dealers Bill 2000. The draft Bill is currently being considered by Parliament. An individual who is licensed to operate as a commercial agent and who may perform the following activities as an agent for others for reward: <ul style="list-style-type: none">– find or repossess for a person any goods or chattels that the person is entitled to repossess under an agreement– collect or request payment of debts– serve any writ, claim, application, summons or other process.
Commercial sub-agent	An individual who is employed by a commercial agent and licensed to perform the duties of a commercial agent.
Computer network	A set of computers that are connected and able to exchange data.

Computer search/inquiry	See 'Command query'.
Computer transaction	See 'Command query'.
Confidential information	Information that is afforded a level of protection, with the lowest level being that for information classified as in-confidence.
Confidential QPS information	Confidential information that is accessible by members of the QPS through the corporate/mainframe computer systems. It includes information owned by other agencies and other police jurisdictions.
Confidentiality	The characteristic of data and information being disclosed only to authorised people, entities and processes in the authorised manner.
Corporate/mainframe systems	Refers to POLARIS and the QPS System used by the Queensland Police Service.
Criminal charge history	See 'Charge record'.
Criminal history	Convictions recorded against a person in respect of offences.
In-confidence information	<p>Sensitive material/information and resources that require a limited degree of protection. Information and resources should be classified as in-confidence when unauthorised disclosure, loss, compromise or misuse of which, or damage to, might possibly:</p> <ul style="list-style-type: none"> – cause harm to the country, government, or legitimate activities of an agency – be prejudicial to the establishment and maintenance of lawful methods for the protection of public safety – cause harm to any person, organisation or local/State/Territory/Federal Government body that provided information to the agency under an assurance and/or expectation of confidentiality or about which the agency holds information – give unfair advantage to any entity (National Police Research Unit 1995). <p>(See appendix A for examples of in-confidence information.)</p>
Incident	An occurrence that has been assessed as having an adverse effect on the security or performance of an information system.
Information system	All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination and disposition of information.

Information-system security	Measures and controls that ensure the confidentiality, integrity and availability of information. It includes hardware, software and information/data being processed, stored and communicated.
Intermediary	The individual who obtains information from the supplier and provides to the end-user.
Member (of the QPS)	An employee of the QPS who is a police officer, staff member or police recruit.
National Exchange of Police Information	A computer system that provides access to cost-effective national information, such the National Names Index and the national automated fingerprint identification system. The system is a joint initiative by the Federal and State Governments, in combination with all Australian police organisations.
Order (QPS definition)	Instruction requiring compliance with the course of action specified. Orders are not to be departed from.
Password	A string of characters containing letters, numbers and other keyboard symbols that is used to authenticate a user's identity or authorise access to data. A password is generally known only to the authorised user who originated it.
Personal information	Information pertaining to someone's personal particulars. Includes factual information, such as address and criminal record, but may also include other types of information, such as political or religious persuasion.
POLARIS	The computerised integrated information system in use by the QPS. The system is constantly being developed and will eventually replace older information systems such as the QPS System. The primary business applications are warrant and offender-history systems.
Policy (QPS definition)	An outline of the QPS attitude regarding a specific subject that must be complied with under ordinary circumstances. Policy may only be departed from if there are good and sufficient reasons for doing so. Members may be required to justify their decision to depart from policy.
Private investigator	Definition as it appears in the Security Providers Act 1993 . A person who is licensed to operate as a private investigator and who, for reward, obtains and gives information about another person.
Procedure (QPS definition)	The general method by which an objective is to be achieved or a task performed, consistent with policies and orders. A procedure may outline actions that are generally undertaken by people or organisations outside the QPS.
Process server	A person who serves process (e.g. summonses).
QPS System	A series of computerised information systems currently in use by the QPS. This is an older system that will eventually be replaced by POLARIS.

QueryMaster Inquiry	A query language facility that enables users to extract data. For this Inquiry it was used as a means of checking audit trails to determine whether any member had conducted a computer check on particular parameters (e.g. by name).
Record of charges	See 'Charge record'.
Risk-based management	A management approach that considers unquantifiable, speculative events as well as probable events (i.e. uncertainty as well as risk).
Risk management	The process of identifying, controlling and minimising and/or eliminating security risks to information systems. The controls or processes introduced to mitigate risk should be at a level commensurate with the value of the assets being protected.
Searches	See 'Command query'.
Standing Order (QPS definition)	An established procedural directive for an organisational unit of the QPS, governing the administrative processes within that unit, consistent with Service policy.
Subject officer(s)	A person(s) who is the subject of an investigation into an allegation of misconduct.
Transaction	See 'Command query'.
User Identification (ID)	Unique symbol or character string used by an information system to recognise a specific user.

EXECUTIVE SUMMARY

The Criminal Justice Commission (CJC) was established by the **Criminal Justice Act 1989**. It has a statutory responsibility to investigate alleged or suspected misconduct and official misconduct by members of the Queensland Police Service and, where appropriate, to offer advice to units of public administration on the detection and prevention of official misconduct.

In August 1998 the CJC received information that officers stationed at the Nerang Police Station may have been unlawfully disclosing confidential information from the Queensland Police Service (QPS) computer systems to a cleaner who was employed at that station. During the course of an investigation into this matter, the CJC received other allegations of police officers unlawfully disseminating QPS information. In addition, there was a steady flow of similar complaints that could not be productively investigated because of issues relating to current QPS information systems. In order to investigate those matters that the CJC could pursue, it was decided to commence an inquiry known as Project Piper.

As the investigation progressed, CJC investigators became more and more suspicious that a significant number of police, particularly at the Nerang Police Station but also elsewhere, were lying to the CJC about their conduct. After careful deliberation, the Commission decided to conduct a public hearing to assist in the productive investigation of these matters. It was also decided to hear three days of public submissions to allow stakeholders to express their views and concerns on the issues revealed during the Inquiry.

The aim of this report is to examine and suggest remedies for issues of concern relating to the type of misconduct revealed during this and previous investigations. It is essentially a report focusing on risk-reduction and risk-prevention methodologies and strategies rather than on the investigative findings of the Inquiry.

The CJC's objective was to develop recommendations aimed at:

- reducing the incidence of misconduct of this nature within the QPS
- modifying QPS information-management systems to improve information security and afford greater protection to information accessible through the computer systems
- ensuring that confidential information is given an appropriate level of protection through legislation.

In developing these recommendations, the CJC considered, in detail, the current policies, procedures and practices of the QPS with regard to the management of information security. This was a large undertaking given that the QPS has been very active in this area (detailed in chapter 5). The purpose of this review was to identify the measures taken by the QPS to preserve the security of information and, by identifying any 'gaps' in the framework of its information-security management, to assist in further reducing the opportunity for this misconduct to occur.

The report is not only concerned with information-security management within the QPS; it also discusses the nature of the market for information, including current government provisions for the release of restricted information and current government legislation to protect confidential information.

The report also suggests proactive strategies that may be of benefit to all government departments and agencies responsible for protecting confidential government information.

The central issues (chapter 2)

Through examination of the relevant research literature and the evidence heard during the Public Inquiry and previous CJC investigations, three central issues became apparent. These provided the framework upon which this report was prepared:

- 1. Information security.** Information security is concerned with the protection of information from a wide range of threats. It is becoming an increasingly important priority for many organisations both nationally and internationally. The Organisation for Economic Co-operation and Development issued information-security principles in 1992. The importance of information security was highlighted by the creation of an Australian and New Zealand Standard on the subject (AS/NZS 4444.1:1999 and AS/NZS 4444.2:1999). Information security is of importance to the QPS for a number of reasons. Firstly, the majority of employees are granted access to computer systems that hold confidential information. Secondly, if privacy legislation were to be introduced, the QPS would need to be in a position where costly changes to work practices and policies would be unnecessary. Thirdly, breaches of information security can compromise the safety of individuals and can ultimately be costly for the QPS. Finally, because there will always be a market for illegally obtained information, the threat to information security is never-ending.
- 2. The market for information and the intermediaries who facilitate information exchange.** The demand for confidential information is created by end-users such as finance organisations and legal firms, whose staff are often trying to locate evasive individuals. Private investigators and commercial agents act as the intermediaries between the end-users and the suppliers of information. Examining the issues of concern in this report required consideration of the market for information.
- 3. Legislation to protect information.** Of particular interest is legislation to protect the privacy of community members and confidential government information. The law as it relates to unauthorised access and release of confidential information is also a matter for consideration.

The investigation (chapter 3)

During the Public Inquiry, five brackets of evidence were presented. Each is described below:

Nerang Police Station: From 1995 to 1998 a number of police officers were frequently accessing information on the QPS computer systems and providing that information to the station cleaner, who in turn passed the information to a private investigator in exchange for a benefit. As a result of preliminary investigations, 53 former and current officers were interviewed by CJC officers. There is persuasive evidence that, of these 53 officers, 17 were involved in hundreds of instances of unlawful access to, and disclosure of, confidential information. One officer in particular was found to have conducted 1777 inquiries on 291 individuals over the three-year period.

The lengthy period during which the misconduct continued at Nerang and the substantial number of officers involved points to a culture of acceptance of the unlawful behaviour among many police at that station. A number of the subject officers stated that the fact that the station cleaner was a former police officer influenced their decision to provide information. One officer even stated: 'We regarded [the cleaner] as one of us; being ex-police, there seems to be that tight-knit circle whether you're ex or whether you're current.' In other evidence, some officers said they felt it was difficult to say no to the cleaner's requests for confidential information because of his apparent 'popularity' and familiarity with the other officers at the station. One officer stated that he was fearful of the repercussions of naming

other officers who were supplying information. Other evidence suggested collusion on the part of some officers in an effort to frustrate the CJC's Inquiry and to avoid punishment.

Of the twelve serving QPS officers who were suspected of providing information to the cleaner (not all of whom appeared before the Inquiry) five have been disciplined and demoted. The remainder are awaiting the outcome of disciplinary action.

Inala Police Station: For the greater part of 1999, the Senior Sergeant who was the Officer in Charge of this station used the QPS computer system to help locate debtors on behalf of a debt-collection agency. This officer was also licensed in Queensland as a private investigator. He had declared to his supervisor that he had secondary employment but described the occupation as a courier driver.

The principal of the collection agency who sub-contracted to the officer indicated that during the period 17 February 1999 to 8 December 1999 the officer was paid a total sum of \$10,039.40 by the agency. Only some of these jobs were discharged with the aid of the QPS computer systems. Investigations suggested that this officer conducted improper searches on 22 people. A significant finding was that several of the searches were conducted under the computer-user identification codes of six other officers stationed with the Senior Sergeant. In evidence, the Senior Sergeant admitted that he did some of the searches using other officers' user identification.

This officer resigned from the QPS; consequently, he cannot be the subject of disciplinary action.

Fortitude Valley Police Station: A Senior Constable at this station was found to have confirmed to an unauthorised person the existence of a domestic-violence order on a woman's restricted computer record. He also released her silent phone number to the unauthorised person. While giving evidence, the woman alleged that she was fearful of the man and that he had stalked her for many years. The woman claimed that she had moved house three times and obtained a silent phone number to evade him. The Senior Constable who released the information was untruthful during two interviews with CJC investigators and did not admit to his actions until he appeared before the Inquiry.

This officer has been disciplined and was demoted from Senior Constable 2.2 to Senior Constable 2.1.

North Queensland Police Station: A Constable who had just graduated from the Academy training program was found to have conducted at least 300 improper computer searches between 4 June 1999 and 18 August 1999. The Constable performed searches on acquaintances and family. He claimed he did the checks out of curiosity and to familiarise himself with the computer systems. Of importance in this case is that the officer had received comprehensive training on the ethical and proper use of QPS computer systems and yet, within weeks of being placed in his first job, used the QPS computer systems for personal reasons.

This officer was disciplined and fined \$450.

Southport Police Station: This investigation was concerned with an allegation that a Constable had released confidential information about a criminal investigation to a person who was a potential suspect for the crime. Evidence was heard that the Constable accessed the crime report several times despite the fact that he was not an investigator on the case. It was also demonstrated that between 12:00 a.m. and 1:00 a.m. on 9 January 1999 the Constable and the potential suspect spoke for 17 minutes during which time the Constable accessed the crime-report details. The Constable had little recollection of the conversation. He admitted to conducting the computer check but denied acting improperly.

This officer has been disciplined and was demoted in rank from Constable 1.6 to Constable 1.1.

The nature of the misconduct (chapter 4)

The CJC has been investigating allegations of improper access and/or release of information since its inception. From these investigations it has become evident that some subject officers have engaged in this form of misconduct with seriously corrupt intentions, while others have done so for other improper reasons. Regardless of the reasons given for improperly accessing and/or releasing information, what is demonstrated by the CJC experience is the ease with which individual members can misuse the QPS computer systems without fear of detection. In the absence of a policy such as a 'reason for transaction' requirement, it is very difficult to enforce accountability.

For some forms of misconduct, reliance is placed on complaints statistics as an approximate estimation of the problem. This provides some assistance in determining the level of response needed to deal with the problem. However, it is clear that complaints statistics should not be relied upon as an accurate measure of prevalence for this type of misconduct, nor should the complaints mechanism be considered a comprehensive system of monitoring and detecting improper access and/or release of confidential information.

The CJC is of the view that factors other than prevalence — such as the potential for abuse and the seriousness of potential harm — should be used to determine what the response should be to this type of misconduct. In addition, the following points are important when considering how to deal with the problematic issues identified during this and previous investigations:

- Though the motivation for committing this type of misconduct may vary, each instance is a breach of trust and of the law, and an invasion of privacy.
- Information accessible on the QPS corporate/mainframe systems is restricted and not generally accessible to the general public.
- The observations of this and previous investigations reveal the potential for abuse of the QPS corporate/mainframe computer systems by members of the Service.
- Restricted information has a market value because it is particularly useful for locating evasive individuals and can provide more information (e.g. criminal-charge history) than found on publicly available databases.
- Given that much of the information available on QPS computer systems relates to individuals in the community, it is important to show the community that it can continue to have confidence in the QPS.
- If no action is taken to solve these problems, there is a risk that organisations with which the QPS shares information may question its capacity to protect confidential information.

The QPS submitted that, when developing the recommendations for this report, the CJC should bear in mind that the QPS budget is limited. The CJC has attempted to ensure that the recommendations are financially realistic and appropriate for the Service. However, it was not possible to make recommendations that are cost-neutral. The CJC is of the view that the issue of budget priorities is one for both the QPS and the Government; the recommendations made are intended to be considered by all agencies and departments affected by them. Just as it is important for the QPS to establish its priorities, it is also necessary for the Government to do so and, as a result, the policy direction it gives to departments and agencies with regard to protecting confidential government information.

Information security in the QPS (chapter 5)

The QPS takes the issue of information security seriously and so has taken a range of initiatives to protect the information available on its computerised information-management systems. In 1993 the QPS established an Information Security Project to develop the Information Security Policy Development Framework. The framework was implemented in September 1998 and covers all areas of information-security management. The QPS has two organisational units responsible for information security — the Information Security Section and the Ethical Standards Command. The latter investigates breaches of information security. An Information Steering Committee and the Risk Management Committee also contribute to information-security management within the QPS.

The QPS has a wide range of policies and procedures in place to enhance information security. These policies and procedures are complemented by corporate computer systems that create full audit trails of all user activity. Audit trails are currently used to deal with technical problems and to assist operational police and the CJC in their investigations. All new members of the Service receive training in information security through either recruit training or induction programs. Civilian members are also required to sign a confidentiality agreement before they are granted access to the computer systems. Awareness of information security among Service members is heightened by warning screens that routinely appear whenever they log onto a computer system holding confidential information.

The QPS is commended on its initiatives to date to improve information security.

Improving information security in the QPS (chapter 6)

Information-security management is becoming an increasingly important priority for organisations. This is not surprising, given that information is recognised as a valuable asset to the organisation. The advent of information technology has resulted in much more efficient information systems, with consequent benefits to productivity. The technology has also facilitated open communication systems between employees.

These rapid advances are accompanied by greater risks to the security of the information. The risks have been exacerbated by the lag in technology to obviate those risks and the delay in organisations' recognition of the need to have strong information-security management. In assessing the QPS information-security management system, all of the following were considered:

- the Australian and New Zealand Standard on Information Security Management (AS/NZS 4444.1:1999) in combination with a review of current literature on best practice in the area
- the issues raised through public submissions and presentation of evidence
- the findings of previous investigations
- the lessons to be learnt from other jurisdictions, particularly the NSW Police Service
- the final comments and submission made by the QPS.

This report has made recommendations that represent both an organisational and a technological response to the issues and problems identified. A significant number of recommendations have been made to 'close any gaps' in policy and procedure (e.g. a policy to prohibit leaving open computer terminals unattended; proper disposal of paper copies of in-confidence material, and mandatory recording of reasons for transactions). The report also recommends that the location of the Information

Security Section be reviewed and consideration given to its placement within the Ethical Standards Command. Technological recommendations for the development of features such as alert monitoring to improve detection systems have also been made. Finally, the report recommends that the QPS give priority to the development and implementation of an ongoing and systematic program of internal audit on access to and use of QPS computer systems. Such a program should have both random and targeted components. This will allow the Service to be proactive when monitoring this type of misconduct.

The CJC is of the view that implementation of these recommendations will complement the information-security initiatives already undertaken by the QPS and deal effectively with the specific security issues revealed during this and previous CJC investigations into this type of misconduct.

Markets for information (chapter 7)

The observations made during this Inquiry were not very different from those made during the ICAC Inquiry into the release of confidential government information (1992a). In the majority of instances, the type of misconduct revealed during this Inquiry was in response to an information request from an unauthorised person. It became apparent that private investigators and commercial agents often serve as the information brokers who obtain information on behalf of clients, the majority of whom are businesses from the private sector.

Within Queensland, confidential information of the type that was of interest to this Inquiry can be lawfully released by CITEC CONFIRM, the QPS Police Information Centre and Queensland Transport, but only in certain circumstances. Each organisation has rules and guidelines on access to restricted databases. CITEC CONFIRM provides information efficiently and at a cost comparable with that seen in the illicit information market. It became apparent that illicit means were used because the individuals and organisations seeking the information would not have been granted access to restricted information under current government policy.

Although some reasons for seeking information were questionable, many appeared to be legitimate (e.g. locating individuals for the purpose of serving legal process and executing court judgments). As a result, the CJC has recommended that the Government review the restrictions that currently apply to accessing criminal histories and particulars on driver's licences and vehicle registrations to determine whether any of them can be varied or waived in certain cases.

Industry regulation in Queensland (chapter 8)

Of particular concern to the CJC are the regulatory requirements for the private-investigator and commercial-agent industries that have a legislative base. The current regime of government regulation is not sufficient for either industry to ensure even the minimum level of professionalism and integrity.

During the writing of this report, the CJC became aware that the Office of Fair Trading has for some time been developing new legislation that will significantly change the regulation of the commercial-agent industry. The CJC was able to consider the draft Property Agents and Motor Dealers Bill 2000, which was released for public consultation on 26 July 2000. The CJC provided the Office of Fair Trading with comments, to which the Director-General of the Department of Equity and Fair Trading responded. In principle, the CJC supports the draft Bill and considers that the Bill will significantly improve government regulation. However, the CJC believes that, on a small number of issues, further amendments should be made to the draft Bill. It is recommended that, in debating the draft Bill, the Government consider the issues raised and comments made in this report.

Government regulation of the private-investigator industry is considerably weaker than that which is being proposed for the commercial-agent industry. Judging from the literature in this area, there is a general consensus that much more could be done to better regulate the industry and bring it up to the required standard. Suggestions for improvement include a mandatory code of conduct, the establishment of a complaints-receiving body, more stringent training requirements and changes to criteria for automatic exclusion. This report has recommended that the Government review the **Security Providers Act 1993** with a view to raising industry standards to the requisite level, thereby ensuring professionalism and integrity.

Information protection and the law (chapter 9)

The final issue raised by the Inquiry concerned current legislation. The CJC is satisfied that legislative provisions for the improper release of confidential government information are adequate. On the issue of improper access to confidential government information by members of the Service, the CJC recommended in chapter 6 ('Improving Information Security in the QPS') that an Order of the Commissioner be promulgated, prohibiting QPS members from unauthorised access to confidential government information. Such an order will provide the necessary grounds on which to commence disciplinary action against a member who cannot demonstrate an official police reason for accessing confidential information. The CJC did not consider it necessary to make improper access to computer systems by authorised members a criminal offence.

It was noted during this Inquiry and the ICAC Inquiry (1992a) that legislation was inadequate for prosecuting those individuals who attempt to procure, receive, obtain or possess confidential government information when a financial benefit paid to the public-sector employee in exchange cannot be demonstrated (if it can be demonstrated, the individual can be charged with official corruption or a similar offence). This was particularly the case for the end-users such as the financial institutions and legal firms, which were one step removed from the initial transaction between the member of the Service and the intermediary. To address this issue, the CJC has recommended that consideration be given to the creation of an offence that prohibits people from obtaining or trying to obtain from government records any confidential information about other people (stored through any medium). The proposed legislation must include a requirement for dishonesty, or knowledge on the part of the person seeking the information that it is confidential.

The final issue that received considerable attention in the public submissions was that of privacy legislation. The issue of privacy is not new in Queensland; in 1998 the Legal, Constitutional and Administrative Review Committee (LCARC) released its report **Privacy in Queensland** and recommended that privacy legislation and a privacy commissioner be introduced. The current Government is reviewing its position on privacy. This report recommends that, as part of that review, the government revisit the LCARC report and, in doing so, give further consideration to the introduction of a Privacy Act based on the Commonwealth model.

Conclusion (chapter 10)

Mindful of its statutory obligations, the CJC is of the view that it must monitor the implementation of the recommendations made within this report. For the recommendations made to the QPS, the CJC favours the establishment of a small QPS Implementation Committee, with representation from the CJC, to oversee the implementation of recommendations that are directly relevant to the QPS. The three recommendations regarding industry regulation of private investigators and commercial agents are a matter for the Office of Fair Trading. Two recommendations of broader government application have been made. It is expected that the CJC will be told which government departments are to have responsibility for their implementation.

Though this report is primarily concerned with the QPS, it would be unfair to suggest that information-security management within the QPS is any looser than that typically seen in other jurisdictions and other areas of government. Therefore the issues raised may also be of interest and the recommendations made of benefit to other government departments and agencies. This report should be of particular interest to any areas of government that store or have access to confidential information for which there may be an illicit market.

The CJC intends to monitor the implementation program continuously and to prepare internal updates regularly. It is the CJC's present intention to produce a follow-up public report on the implementation of all recommendations in two to three years' time. In addition, the CJC may report on the progress of implementation in its Annual Report, its reports to the Parliamentary Criminal Justice Committee, its research and prevention reports, and the QPS Monitor.

List of recommendations

RECOMMENDATION 6.1 — ENHANCING THE CORPORATE RESPONSE TO INFORMATION SECURITY **P. 55**

- 6.1.1 That the Queensland Police Service, through the establishment of an information-security committee, or through current committee structures, ensure that the following duties are discharged on an ongoing basis:
- review and approve information-security policy and overall responsibilities
 - monitor significant changes in the exposure of information assets to major risks
 - review and monitor incidents involving information security
 - recommend, to the Commissioner of Police, major initiatives to enhance information security.
- 6.1.2 That, as a matter of priority, orders, policies and procedures for information security be finalised and released to members of the Queensland Police Service.

RECOMMENDATION 6.2 — REVIEW LOCATION OF THE INFORMATION SECURITY SECTION **P. 56**

That the Queensland Police Service review the organisational structure as it relates to information security, giving particular consideration to the placement of the Information Security Section within the Ethical Standards Command so that the information-security goals and objectives of the Queensland Police Service can be more readily achieved. As part of this review, the functions of the Information Security Section should also be considered to determine whether or not they are grouped together appropriately.

RECOMMENDATION 6.3 — PREVENTING INAPPROPRIATE ACCESS TO QUEENSLAND POLICE SERVICE COMPUTER SYSTEMS **P. 58**

- 6.3.1 That the Queensland Police Service communicate, through an Order, that:
- authorised users are not permitted to access any computer system unless they do so as part of their official duties (such duties being those actions that a person is authorised to perform as a member of the Queensland Police Service)
 - members are not entitled to access any computer system merely by virtue of their status, rank, office or level of authorised access.
- 6.3.2 That the Queensland Police Service formally provide members with specific examples of appropriate and inappropriate reasons for access. The examples should include the inappropriate reasons proffered by members who have come under investigation for accessing of police computer systems.

RECOMMENDATION 6.4 — PREVENTING USE OF ANOTHER USER-ID **P. 59**

- 6.4.1 That the Queensland Police Service develop and implement an order that requires users to always log out of the computer system if they have to leave their computer terminal unattended.
- 6.4.2 That the Queensland Police Service develop and implement an order prohibiting access to computer systems by means of another person's user-ID.
- 6.4.3 That, in developing any future standard desktop-operating environment, the Queensland Police Service give careful consideration to mandatory use, where appropriate, of a 'lock screen' or equivalent facility at the desktop level (e.g. for those members who are allocated their own personal computer).

RECOMMENDATION 6.5 — RISK MANAGEMENT TO ENSURE THAT MEMBERS LOG OUT **P. 60**

That, as part of risk management at the district and local levels, officers-in-charge and supervisors ensure compliance with the requirement to log out of computer systems before leaving a terminal unattended.

RECOMMENDATION 6.6 — PREVENTING CONFLICT OF INTEREST THROUGH OUTSIDE EMPLOYMENT **P. 60**

That the Queensland Police Service promulgate an order:

- prohibiting members from being registered and/or licensed as a private investigator, commercial agent or sub-agent, and/or process-server
- prohibiting members from undertaking employment with any private-investigation, process-serving or other agency/organisation that is concerned with locating people or obtaining personal and/or confidential information.

The only exception to the above order should be for those members who obtain the formal authorisation of the Deputy Commissioner of Police to engage in this type of secondary employment after applying to establish that theirs is a special case.

RECOMMENDATION 6.7 — ADDRESSING THE ISSUE OF ASSOCIATIONS BETWEEN POLICE OFFICERS AND PRIVATE INVESTIGATORS OR PEOPLE IN SIMILAR OCCUPATIONS. **P. 61**

That the Ethical Standards Command of the Queensland Police Service, in consultation with the Criminal Justice Commission, review the issue of associations between police officers and private investigators, or individuals in similar occupations, to determine policies and strategies to deal with the issue effectively and provide guidelines for police officers on what kind of association is appropriate.

RECOMMENDATION 6.8 — ENSURING THE APPROPRIATE DISPOSAL OF PAPER COPIES OF IN-CONFIDENCE INFORMATION **P. 62**

- 6.8.1 That the Queensland Police Service formally provide guidelines, with examples, on how information from the computer systems should be classified to ensure that members understand which disposal methods are appropriate for paper copies containing this type of information.
- 6.8.2 That the warning screens for the access to Queensland Police Service corporate/mainframe computer systems include a condition that all information in these computer systems has a minimum classification of in-confidence unless otherwise specified, and that hard-copy print-outs should be disposed of in accordance with current QPS policies.
- 6.8.3 That an in-confidence notice be inserted on each computer screen that may contain in-confidence information within the Queensland Police Service corporate/mainframe systems to ensure that the in-confidence classification is included on all printed hard copies.

RECOMMENDATION 6.9 — TECHNOLOGY FOR INFORMATION SECURITY **P. 64**

- 6.9.1 That, as a matter of priority, the Queensland Police Service progressively incorporate information-technology capabilities within the next three years to:
- install an ‘alert’ monitoring feature for selected records and transactions
 - install a ‘barring-access’ function for selected records and information
 - develop and implement a system for detecting excessive transactions by authorised users.
- 6.9.2 That, as part of strategic planning, the Queensland Police Service continues to monitor the development of new IT capabilities that can assist in the protection of information and the detection of inappropriate use.

RECOMMENDATION 6.10 — SYSTEMATIC AND ONGOING INTERNAL AUDIT **P. 66**

- 6.10.1 That the Queensland Police Service give higher priority to the use of audit strategies to prevent this type of misconduct by developing and implementing a systematic and ongoing internal audit program, which is both random and targeted, of access to and use of the computer corporate/mainframe systems.
- 6.10.2 That, as part of the risk-management process, managers and supervisors incorporate a program of local internal audit of access to and use of computer corporate/mainframe systems.

RECOMMENDATION 6.11 — REASON FOR TRANSACTION **P. 71**

- 6.11.1 That the Queensland Police Service order that all members must record a reason for access for each transaction made on the corporate/mainframe computer systems, either through mandatory computer entry, police notebook entry, or some other systematic documentation process, except where:
- a series of transactions are logically linked, in which case a single reason for the multiple transactions will afford an appropriate level of accountability
 - where other official police documents provide evidence of an appropriate reason for the transaction
 - where the duties of an officer require an unusually high number of transactions in relation to information that would routinely be accessed (e.g. a traffic police officer performing vehicle registration checks).
- The last proviso should not apply to those members accessing sensitive information, such as intelligence databases.
- 6.11.2 That, where transactions are conducted on behalf of another member, the requesting member be required to record a reason for the request through mandatory computer entry, police notebook entry, or some other systematic documentation process.
- 6.11.3 That, where transactions are performed on behalf of another member, the person conducting the transaction asks the requesting member the reason for their request and their name, and records that information through mandatory computer entry, police notebook entry, or some other systematic documentation process.

RECOMMENDATION 6.12 — RAISING AWARENESS OF INFORMATION SECURITY AND INDIVIDUAL ACCOUNTABILITY **P. 74**

- 6.12.1 That, in response to this report, the Commissioner of Police issue a notice to all members, addressing the issues arising from this Inquiry, areas of concern and policy developments in respect of information security.

- 6.12.2 That the Queensland Police Service require all members to sign an acknowledgment stating that they:
- agree to the information-security policies as specified
 - fully understand that the QPS computer system is not for personal use and therefore should only ever be accessed and used in the performance of official police work
 - have read the legislation and will abide by the legislation, orders, policy and procedural rules and guidelines on computer use and access, and release of information
 - understand that a breach of the terms of the contract/agreement will result in criminal and/or disciplinary action and possibly dismissal.
- To ensure that no significant administrative burden is placed on the QPS, implementation should be progressive and be applicable to all new recruits from January 2001.
- 6.12.3 That a supervisor or manager witness the signing of the acknowledgment, and also attest that the member has demonstrated that he/she has read the contract/agreement and fully understands its content.
- 6.12.4 That, where a supervisor or manager is not satisfied that a member has the necessary understanding of legislation, orders, policies and procedures relating to security of computer information, access should not be granted until the member completes appropriate training and education
- 6.12.5 That all members be required to re-sign their acknowledgment when they request new, changed or renewed access to a mainframe/corporate system or database

RECOMMENDATION 6.13 — EXTENDING INFORMATION SECURITY **P. 76**

- 6.13.1 That the Queensland Police Service incorporate, in higher education and training programs, particularly those catering for supervisors and managers, training sessions/modules on computer use, information security, and supervision of computer use by subordinates.
- 6.13.2 That the Queensland Police Service educate managers and supervisors on the application of the principles of risk management to develop processes for the effective monitoring and supervision of subordinate staff in the use of and access to the police computer system.
- 6.13.3 That the Queensland Police Service complete the development of the Competency Acquisition Program module on computer use and information security.

RECOMMENDATION 7.1 — ACCESS TO CRIMINAL HISTORY, DRIVER'S-LICENCE AND VEHICLE-REGISTRATION RECORDS **P. 90**

That the Government should review the restrictions that currently apply to accessing criminal histories, and driver's licence and vehicle-registration particulars, to determine whether any of those restrictions can be varied or waived in certain cases.

RECOMMENDATION 8.1 — GOVERNMENT CONSIDERATION OF CJC COMMENTS ON THE DRAFT PROPERTY AGENTS AND MOTOR DEALERS BILL 2000 **P. 101**

That the Queensland Government, which will soon debate the draft Property Agents and Motor Dealers Bill 2000, give serious consideration to the issues raised and the suggestions made within this report to further improve the regulatory control to be afforded by the new legislation.

RECOMMENDATION 8.2 — GOVERNMENT REVIEW FOR THE BETTER REGULATION OF THE SECURITY INDUSTRY **P. 103**

That the Queensland Government commence a review of the **Security Providers Act 1993** and industry regulation within the next twelve months. The review should aim to develop legislation to provide a regulatory environment that is comprehensive and that ensures that the professionalism and integrity of the security industry are strengthened.

RECOMMENDATION 8.3 — AMENDMENTS TO THE SECURITY PROVIDERS ACT 1993 **P. 104**

- 8.3.1 That, as a matter of urgency, the **Security Providers Act 1993** be amended to allow the chief executive officer to consider the suitability of an applicant or current licence-holder where that person has been found guilty of a disqualifying offence.
- 8.3.2 That, as part of the government review of legislation and industry regulation, the suitability of current disqualifying offences and the disqualifying period be reconsidered.

RECOMMENDATION 9.1 — MAKING IT AN OFFENCE TO OBTAIN OR TRY TO OBTAIN FROM GOVERNMENT RECORDS ANY CONFIDENTIAL PERSONAL INFORMATION ABOUT ANY OTHER PERSON, HOWEVER IT MAY BE HELD **P. 108**

That consideration be given to the creation of an offence that prohibits people from obtaining or trying to obtain from government records any confidential personal information about others, however it may be held. The proposed legislation must include a requirement for dishonesty on the part of the person seeking the information, or his/her knowledge that the information is confidential.

RECOMMENDATION 9.2 — GOVERNMENT RESPONSE TO THE EMERGING ISSUES OF PRIVACY AND INFORMATION PROTECTION **P. 109**

That the Queensland Government, when reviewing its position on information privacy, revisit the recommendations made in the report of the Legal, Constitutional and Administrative Review Committee (LCARC), **Privacy in Queensland**, and in doing so, give further consideration to the introduction of a Privacy Act based on the Commonwealth model.

INTRODUCTION

The protection of confidential and personal information collected by government agencies and departments has emerged as an important and often controversial issue, both nationally and internationally. Within Australia, numerous agencies and groups have expressed their interest in this issue by way of investigative and/or public reports, media articles and reports, and other documents such as the Australian and New Zealand Standard on Information Security Management (AS/NZS4444.1:1999, AS/NZS 4444.2:1999). This is also an area of increasing community concern, as it is often the personal and private details of community members that are at risk.

As new information system technologies and initiatives are adopted in the public sector, a growing number of public servants have acquired the capacity to access the massive amounts of confidential information available on integrated computer systems. Such advances greatly assist government departments and agencies in the delivery of services to the community, and in making their internal operation more efficient. However, with these advances come new and emerging risks. It is important that these risks are effectively managed and that appropriate risk-reduction strategies are adopted to minimise the chance of confidential information being misused.

This chapter begins with a description of the scope of the report. This is followed by a section outlining the statutory powers and responsibilities of the CJC to investigate and report on 'misconduct' and 'official misconduct', and to provide advice and/or assistance to law-enforcement agencies on the detection and prevention of official misconduct. The next section describes the genesis of this investigation and the background leading to the Public Inquiry. The final section sets out the structure of the report.

SCOPE OF REPORT

This report has resulted from the CJC's Inquiry into alleged improper access to, and release of, confidential and personal information from the police computer systems by members of the Queensland Police Service (QPS).

The aim of the report was to examine and suggest remedies for the issues of concern relating to this type of misconduct, as revealed during this and previous investigations. It is essentially a report focusing on methods of risk-reduction and risk-prevention rather than a report of the investigative findings of this Inquiry.

The CJC's objective was to develop recommendations aimed at:

- reducing the incidence of misconduct of this nature within the QPS
- modifying QPS information-management systems to improve information security and afford greater protection to information that is accessible through the corporate/mainframe computer systems
- ensuring that the personal and confidential information is given an appropriate level of protection through legislation.

To achieve this objective, the CJC was required to review, in detail, the current policies, procedures and practices of the QPS with regard to information-security management. This was a significant undertaking given that the QPS has been very active in this area (detailed in chapter 5). The purpose of this review was to identify the measures taken by the QPS to preserve information security and, by identifying any 'gaps' within the framework of its information-security management, to assist in further reducing the opportunity for this misconduct to occur.

The report is not only concerned with information-security management within the QPS; it also considers the nature of the market for information and examines current government provisions for the release of restricted

information, and current legislation designed to protect confidential information held by government agencies.

The QPS similarly recognised the need for a strategic approach to the issues of concern, and stated its position in its written submission (2000, p. 5):

The Service is acutely aware of the need to implement policies and practices designed to maintain the security of its information. The issue is where to strike the balance between establishing practices that may unduly impede the work of operational police while ensuring that systems are in place to protect information against unauthorised access. This problem is not unique to the Queensland Police Service; public and private organisations at the local, state, national and international levels face similar issues. Over the past decade the Service developed security practices and policies as its technological capabilities increased. In many areas, the Service operates at levels not exceeded elsewhere in Australia. It is likely that in the current decade technology may develop as rapidly as it did in the 1990s. Organisations will be required to invest significantly. Security issues will not be solved by a single program or policy and an adaptable and multi-pronged approach will be called for.

The recommendations in this report represent the adaptable and multi-pronged approach that the QPS has called for. They cover policy, practice, procedure and legislation, and are considered to be workable and realistic.

CJC JURISDICTION

The CJC was established pursuant to the **Criminal Justice Act 1989** (the Act), which prescribes its role and statutory obligations. As it is a creation of statute, the CJC may only do that which is authorised by statute. It follows that there must be some statutory basis for this investigation and the recommendations that the CJC has made in this report.

The broad responsibilities of the CJC

Section 23 (f) of the Act provides that the responsibilities of the Commission include in discharge of such functions as, in the Commission's opinion, are not appropriate to be discharged, or cannot be effectively discharged, by the Police Service or the agencies of the State, undertaking:

- (i) research and coordination of the processes of criminal law reform;

- (ii) matters of witness protection;
- (iii) investigation of official misconduct in units of public administration.

Section 3A(1)(d) of the Act provides that the QPS is a unit of public administration.

The Official Misconduct Division and investigation

Section 19(1) of the Act establishes the Official Misconduct Division (OMD) within the CJC. The OMD is the investigative unit [s. 29(1)] and operates on its own initiative, as well as in response to complaints or information received about misconduct [s. 29(2)]. Section 29(3) of the Act sets out the functions of the OMD:

- (a) to investigate the incidence of official misconduct generally in the State; and ...
- (d) to investigate cases of —
 - (i) alleged or suspected misconduct by members of the police service; or
 - (ii) alleged or suspected official misconduct by persons holding appointments in other units of public administration;

that come to its notice from any source, including by complaint or information from an anonymous source; and

- (e) to offer and render advice or assistance, by way of education or liaison, to law enforcement agencies, units of public administration, companies and institutions, auditors and other persons concerning the detection and prevention of official misconduct.

The CJC's jurisdiction in respect of officers in units of public administration other than the QPS is confined to those more serious cases that may constitute official misconduct. The CJC's jurisdiction to investigate is broader in respect of members of the QPS as it can investigate 'misconduct' as well as 'official misconduct'.

Section 32(1) of the Act defines 'official misconduct' as:

- (a) conduct of a person, whether or not the person holds an appointment in a unit of public administration, that adversely affects, or could adversely affect, directly or indirectly, the honest and impartial discharge of functions or exercise of powers or authority of a unit of public administration or of any person holding an appointment in a unit of public administration; or

- (b) conduct of a person while the person holds or held an appointment in a unit of public administration —
 - (i) that constitutes or involves the discharge of the person's functions or exercise of his or her powers or authority, as the holder of the appointment, in a manner that is not honest or not impartial; or
 - (ii) that constitutes or involves a breach of trust placed in the person by reason of his or her holding the appointment in a unit of public administration; or
- (c) conduct that involves the misuse by any person of information or material that the person has acquired in or in connection with the discharge of his or her functions or exercise of his or her powers or authority as the holder of an appointment in a unit of public administration, whether the misuse is for the benefit of the person or another person;

and in any such case, constitutes or could constitute —

- (d) in the case of conduct of a person who is the holder of an appointment in the unit of public administration — a criminal offence, or a disciplinary breach that provides reasonable grounds for termination of the person's services in the unit of public administration; or
- (e) in the case of any other person — a criminal offence.

Insofar as members of the QPS are concerned, the term 'misconduct' is defined in s 1.4 of the **Police Service Administration Act 1990 (PSAA)** as conduct that:

- (a) is disgraceful, improper or unbecoming an officer; or
- (b) shows unfitness to be or continue as an officer; or
- (c) does not meet the standard of conduct the community reasonably expects of a police officer.

Authorisation to conduct hearings

The CJC is authorised to conduct a hearing in relation to any matter relevant to the discharge of its functions and responsibilities, and may receive evidence orally or in writing, on oath or affirmation, or by way of statutory declaration [s. 25(1)].

A person may be summoned to attend before the CJC to give evidence in relation to the subject matter of the Commission's investigation [s. 74(1)(a)] and to produce a record or thing specified in the summons [s. 74(1)(b)].

The Act provides that a hearing of the CJC is to be closed to the public unless the CJC orders, whether before or during the hearing, that it be open to the public [s. 90(1)]. Pursuant to s. 90(2) the CJC may order that the hearing be open to the public only if it considers that:

- (a) the hearing is of an administrative nature; or
- (b) a closed hearing would be unfair to a person or contrary to the public interest.

A person giving evidence before the CJC is not entitled:

- (a) to remain silent with respect to any matter that in the Commission's opinion is relevant to the Commission's investigation if the Commission requires the person to give evidence with respect to that matter;
- (b) to fail to answer a question relating to any such matter that the Commission requires the person to answer;
- (c) to fail to produce any record or thing that, in the Commission's opinion, is relevant to the Commission's investigation, if the Commission requires the person to produce it;

on the ground that to comply with the requirement would tend to incriminate the person [s. 94(2)].

This provision is designed to enable the CJC to get to the truth of the matter under investigation. However, the witness is protected by s. 96(1) of the Act, which provides that a statement made by a witness before the CJC, after he/she has objected to making the disclosure on the ground that it would tend to incriminate the person, is not admissible as evidence against the witness in civil or criminal proceedings in a court, or in disciplinary proceedings.¹

Reports of the CJC

The CJC may resolve to publish a report signed by the Chairperson which, pursuant to s. 26(1) of the Act, shall be furnished to the:

- Chairperson of the Parliamentary Criminal Justice Committee
- Speaker of the Legislative Assembly
- Minister.

Accordingly, the CJC has resolved that this report be furnished to the Queensland Parliament under s. 26 of the Act.

Section 33(1) provides that the Director of the OMD shall report on every investigation that it undertakes (other than by or on behalf of the Complaints Section). A report of the Director shall be made to the Commission or, at the Commission's discretion, to the Chairperson (s. 33(2)). In certain cases the CJC may also furnish a report to the appropriate principal officer in a unit of public administration, so that disciplinary action can be taken on the matter to which the report relates (s. 33(2A)(g)). The CJC has produced reports on each of the subject officers of this Inquiry to the Commissioner of the QPS as the principal officer.

GENESIS OF INVESTIGATION AND BACKGROUND TO INQUIRY

In August 1998 the CJC received information that officers stationed at the Nerang Police Station may have been unlawfully disclosing confidential QPS information to a cleaner who was employed at that station. It was alleged that the cleaner was in turn passing the information to a private inquiry agent.

As a result of receiving the information, the CJC commenced preliminary inquiries, which led to an investigation code-named Operation Herron. This investigation suggested that a large number of QPS officers at the Nerang Police Station had unlawfully accessed the QPS computer systems and disclosed confidential information.

During the course of Operation Herron, other allegations were received by the CJC concerning the unlawful dissemination of confidential information available on QPS computer systems. Such was the volume of the material that the CJC resolved to commence Project Piper, under the umbrella of which all of the allegations were to be investigated. The matters investigated during Project Piper, in addition to the Nerang matter, were:

- a police officer stationed at the Inala Police Station used the QPS computer system to assist him in locating debtors on behalf of a debt-recovery agency (December 1998)
- a police officer at the Southport Police Station obtained confidential information about a QPS investigation from the QPS computer system and provided the information to a person who was a potential suspect in that investigation (January 1999)

- a police officer at a North Queensland Police Station conducted hundreds of searches on the QPS computer system for personal reasons (August 1999)
- a police officer at the Fortitude Valley Police Station obtained the silent number of a woman from the QPS computer system and provided it to a man who she said had been stalking her over many years (September 1999).

In addition, there was a steady flow of similar complaints that could not be productively investigated. This issue is discussed further on pages 28–29.

As the investigation progressed, an increasing concern was that a significant number of police, not just at the Nerang Police Station but elsewhere too, were suspected of lying to the CJC about their conduct. This had the effect of frustrating the CJC's inquiries and demonstrated a willingness by some officers to try to 'tough out' the investigations.

The Commission resolved that, in view of the apparent willingness of many of the officers under investigation to lie, the only way to investigate these matters productively was at a hearing. The remaining issue was whether to hold the hearing in closed session or in public.

The decision to hold a public hearing

To determine whether a hearing should be open, the Commission must consider whether a closed hearing would be unfair to anyone or contrary to the public interest. The test is therefore whether the reasons for conducting a public hearing outweigh those against to such an extent that it would be contrary to the public interest to proceed in private. The CJC considered the experience of the ICAC in a similar case (see appendix B) and sought advice from Mr R A Mulholland QC (appendix C) as to whether the circumstances of this matter would permit a public hearing pursuant to the provisions of the Act. Mr Mulholland QC concluded:

The factors which may be said to be in favour of a public hearing in the current investigation are as follows:

- The unauthorised disclosure of confidential information by police is a serious issue which has not been properly or adequately addressed by the QPS;
- Evidence has been uncovered of widespread misuse of the QPS database for unofficial purposes by police officers and others;

- Despite extensive investigation (including closed hearings) unearthing a substantial amount of evidence, there is good reason to suspect that many QPS officers have lied during the course of disciplinary interviews and this is constituting a serious impediment to the progress of the investigation;
- The Commission believes that public, as opposed to private, hearings provide the most effective method of advancing the current investigation because public examination is more likely to encourage witnesses (specifically the QPS officers who have so far lied) to tell the truth, generate public information and submissions germane to the investigation and, ultimately, provide the best opportunity for ascertaining the truth and helping to eliminate or reduce unauthorised disclosures by police.

Whilst the above are factors for the Commission to weigh and consider, in my view taken as a whole the circumstances are sufficient to warrant a conclusion that to rely exclusively on closed hearings would be contrary to the public interest. It follows from what I have said that I do not regard it as a necessary pre-requisite for public hearing that the investigation will 'fail' without them. However, I repeat my view that the Commission should approach its determination conscious of the legislative intention that extends paramountcy to the protection of an individual's reputation.

In determining where the public interest lies, the potential damage to an individual's reputation by holding a public hearing was therefore a dominant factor. In this context, s 88 of the Act is also relevant. It provides that the CJC may prohibit the publication of evidence identifying a witness if it considers that publication would be unfair to a person. Non-publication of such details can greatly reduce the extent of any damage to an individual's reputation.

On 21 December 1999 the Commission resolved that hearings should be held for the purpose of investigating alleged unauthorised access to, and release of, confidential information from the QPS computer systems by members of the QPS. The Commission authorised the Chairperson to conduct public hearings and, as required, closed hearings, having regard to s. 90 of the Act.

On 27 January 2000 the CJC publicly announced the Inquiry (see appendix D) and called on all interested groups and individuals to make

submissions to it. The Inquiry opened on 14 February 2000, during which a statement from the Commissioner of Police was read endorsing the CJC's Inquiry:

I would like to state from the outset that the Queensland Police Service fully supports the establishment of this Public hearing by the Criminal Justice Commission ... Over the past few years the Service has experienced substantial change and many new challenges, not least of which have been the advances in information technology and the increases in information availability it offers. These technological developments are presenting new opportunities as well as risks to all governments, government agencies, non-government organisations and private individuals in the handling of confidential information. It is therefore timely to examine the conduct of the Queensland Police Service in its handling of confidential information. (CJC unpub., pp. 5–6)

The Chairperson invited submissions from Counsel Assisting the CJC, Mr R P Devlin, and from Mr S Zillman, the Counsel appearing on behalf of a number of police witnesses who had been summoned to appear before the CJC. Mr Devlin gave a detailed account of the evidence that was expected to be given at the hearing, and what might be achieved through a public-hearing process. In his account, he submitted that public interest favoured the evidence being given in public. Mr Zillman made no submissions on this issue but did seek a prohibition on the publication of details that may have identified those police witnesses for whom he was appearing. That issue was dealt with at a later time.

The Chairperson concluded that it was contrary to the public interest to hold the hearing in private. His principal reason for this conclusion was that a public hearing provided a better opportunity than a closed hearing to ascertain the truth, and for determining the true extent of the misuse of the QPS database. As far as damage to an individual's reputation was concerned, this was not a case involving high-profile individuals whose reputations would be damaged by the mere fact of their names being mentioned in association with the hearing. However, where unfairness may have arisen from the publication of a name, an order suppressing those details would ordinarily negate that unfairness.²

The investigative hearings were conducted from 21 February to 1 March 2000. Chapter 3 ('The Investigation') details the observations and evidence heard during this phase of the Inquiry. On 6 March 2000 the CJC commenced three days of public appearances to hear the views of

interested stakeholders and the issues of concern to them.³ The purpose of receiving submissions and inviting public appearances was to encourage informed debate on the issues of concern. It provided an appropriate forum for stakeholders to be heard, and the opportunity for them to make suggestions to improve strategies and systems to protect confidential and personal information. The information from the public submissions and appearances was used to assist in the development of the comprehensive set of recommendations made in this report.

STRUCTURE OF THE REPORT

Chapter 2 describes the central themes that emerged during the Inquiry, and in turn provide the framework for this report. The themes include information security, the market for information, and legislation to protect information. A brief background and description of each theme is given.

Chapter 3 details each bracket of evidence heard during the investigative hearings. The background for each bracket is provided, as well as a description of the evidence as it was revealed during the hearings. At the end of each bracket, the course of disciplinary action taken by the QPS with regard to each of the subject officers is stated.

Chapter 4 discusses the nature of this type of misconduct. The factors considered by the CJC when deciding whether or not to release a public report are outlined.

Chapter 5 describes information security within the QPS. It covers organisational structures, policies and procedures, and features of information technology that improve information security.

Chapter 6 highlights each area where the CJC is of the view that improvements to QPS information security can reduce the opportunity for improper access and/or release of confidential information. A number of recommendations are made to improve information security.

Chapter 7 describes the market for information as observed during the Inquiry. Of particular interest is the structure of the market and why it exists. The systems in place within Queensland to provide access to government information are described. Consideration is given to whether these systems can be improved to reduce market demand.

Chapter 8 is concerned with industry regulation for commercial agents and private investigators. Consideration is given to whether industry

regulation is sufficient to ensure that there is a desirable level of professionalism and integrity in each occupation.

Chapter 9 considers legislative provisions to protect information and to deter improper access to and/or release of confidential information. The areas considered are legislation for improper access to information, improper disclosure, improper attempts to obtain or be in receipt of confidential information, and privacy.

Chapter 10 briefly outlines the conclusions of the report and sets out the processes for monitoring the implementation of recommendations made in this report. The lessons for all government departments and agencies are discussed.

CONCLUSION

The aim of this report was to examine and suggest remedies for the factors that contributed to the type of misconduct revealed during this and previous investigations into improper access and release of confidential information by QPS members. It is essentially a report of risk-reduction and risk-prevention methodologies and strategies rather than a report of the investigative findings of the Inquiry.

The CJC's objectives were to develop recommendations aimed at:

- reducing the incidence of misconduct of this nature within the QPS
- modifying QPS information-management systems to improve information security and afford greater protection to the information that is accessible through the computer system
- ensuring that personal and confidential information is given an appropriate level of protection through legislation.

This report is structured to discuss the range of issues and problems revealed during this and previous Inquiries. The chapters cover information security within the QPS, the market for information, industry regulation for commercial agents and private investigators and the adequacy of legislation in dealing with the issues raised. The proactive strategies recommended in the report may also be of benefit to all government departments and agencies responsible for protecting confidential government information.

THE CENTRAL ISSUES

It became apparent while reviewing the relevant literature and during the course of the public hearing that there are three central issues relating to this type of misconduct. These three central issues provided the framework upon which this report was prepared:

1. information security
2. the market for information and the intermediaries who facilitate information exchange
3. legislation to protect information.

These issues are discussed in this chapter. The first section describes best practice in information security and explains why information security should be a high priority for the QPS. The next section describes the market for confidential information and the intermediaries and end-users who participate in the market. Next, a brief historical account is given of the emergence of the issues of privacy and personal information-protection, to highlight their importance, not just to the QPS, but to all organisations in both public and the private sectors.

WHAT IS INFORMATION SECURITY?

Information security concerns the protection of information from a wide range of threats. It is becoming an increasingly important priority for many organisations. Within private-sector institutions such as banking and finance, information security has been a high priority for some time. Though not as advanced as the private sector, public-sector organisations are also realising the growing importance of comprehensive security for one of their most valuable organisational assets — information.

Over the last several years, many bodies with the responsibility of overseeing the ethical functioning of public-sector organisations within Australia have conducted reviews and investigations relating to information security, and a significant number have made recommendations to improve information-security systems within government. Examples of

such recommendations are to be found in the reports of the Australian National Audit Office, the Commonwealth Ombudsman, the NSW Ombudsman, and the Independent Commission Against Corruption (ICAC).⁴

On the international front, considerable attention is being given to information security. In 1992 the Organisation for Economic Co-operation and Development (OECD) released **Guidelines for the Security of Information Systems**. The objective of information-security systems is defined as ‘the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity’ (p. 4). As shown in table 2.1 on page 8, the guidelines list nine principles important for effective information security.

More recently, the United States Government has taken the position that a national approach is necessary to handle information-security issues within its federal agencies. This stance was prompted by the finding that, despite advances in information technology, there continued to be consistent and serious weaknesses in information security. The Critical Infrastructure Assurance Office (2000) has been established to assist in the development of a national plan for protecting the country’s critical information infrastructure and to coordinate implementation efforts. A national approach was considered the best option because the infrastructure is not contained within state boundaries, but is interconnected across the country.

Organisations implement information-security systems to protect a valuable asset and to meet their goals. The objectives outlined in table 2.2 on page 9 may be appropriate for a unit of public administration.

Recently an Australian and New Zealand Standard⁵ on this issue has been created (AS/NZS 4444.1:1999 and AS/NZS 4444.2:1999). The content of the standard was developed and reviewed by a number of major organisations and committees in the UK and Europe and is aligned with the requirements of the British Standard to

Table 2.1 — Information-security principles issued by the OECD (1992)

PRINCIPLE	
1. Accountability	The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.
2. Awareness	In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.
3. Ethics	Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.
4. Multidisciplinary	Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.
5. Proportionality	Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.
6. Integration	Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.
7. Timeliness	Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.
8. Reassessment	The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.
9. Democracy	The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

Source: OECD 1992

facilitate international business and trade. The rationale for having a standard for information-security management was explained in this way:

With increasing electronic networking between organizations there is a clear benefit in having a common reference document for information security management. It enables mutual trust to be established between networked information systems and trading partners and provides a basis for the management of these systems between users and service providers. (AS/NZS 4444.1:1999 p. iii)

This observation applies equally to law-enforcement agencies, which not only access other government systems (such as transport) but also share information with one another through networks such as the National Exchange of Police Information (NEPI), the Transport Registration and Integrated Licensing System (TRAILS) and the Australian Criminal Intelligence Database (ACID).

In June 2000, Standards Australia⁶ released a new guide on information-security risk management in response to community and industry need. The recent and rapid development of the above standards highlights the growing importance of

Table 2.2 — General information-security objectives for a unit of public administration

-
- Maintain stakeholder confidence in the organisation’s efficiency and trustworthiness.

 - Protect confidential information from inappropriate access and/or disclosure.

 - Prevent members of the unit disclosing information inappropriately, and so avoid liability for the criminal acts that such disclosure constitutes.

 - Ensure that the organisational computer network and data resources are not misused or wasted.

 - Ensure that the organisation operates efficiently, productively and successfully.

 - Avoid expensive and disruptive incidents.

 - Comply with relevant laws and regulations.

information-security management. According to the Information Security Management Standard (1999 4444:1), information security is characterised as the preservation of:

- a) confidentiality: ensuring that information is accessible only to those authorized to have access;
- b) integrity: safeguarding the accuracy and completeness of information and processing methods;
- c) availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met. (p. vii)

Effective information security can only be developed by identifying security requirements through risk assessment and by giving consideration to all legal, statutory, regulatory and contractual requirements and to the principles, objectives and requirements for information processing necessary to support the operation of the organisation.

The critical features of an effective system of information-security management, as outlined in the Standard, include or address:

- an appropriate information-security infrastructure
- asset classification and control
- personnel security

- physical and environment security
- the correct and secure operation of information-processing facilities
- access control
- the inclusion of security provisions in all information systems
- compliance with criminal and civil law, statutory, regulatory or contractual obligations and security requirements.

Information security is concerned with all information held by an organisation and therefore includes information held in media other than computer systems. It is also concerned with other features of security such as asset classification and physical and environmental security. Clearly some aspects of information security are not of interest to the CJC in this report.

The areas of information security that are of interest to the CJC are organisational and technological policies and practices relating to access to, and use of, the confidential government information available to the QPS, particularly through the computer systems. It is the internal threat that is of greatest concern here (as opposed to those emanating from outside the QPS, such as computer hackers).

In assessing information-security management within the QPS, the principles and guidelines outlined above were applied and considered. Chapter 5 outlines information-security management within the QPS, and chapter 6 states the recommendations made by the CJC to improve information-security management within the QPS as it relates to the improper access to, and/or release of, confidential information held on the QPS corporate/mainframe computer systems. The development of recommendations

has been based on risk assessment, models of best practice as described in the relevant standards, the practices of other jurisdictions, the evidence and submissions heard during the public hearing and the experience of prior CJC investigations.

Why is information security and protection important to the QPS?

Advances in information technology have given rise to faster and more efficient information-management systems and facilitated significantly greater sharing of information between departments, governments and, where appropriate, private-sector businesses. They have also improved the speed and efficiency of services offered by the Government. Increasingly, the Government is using initiatives in information technology and management to improve service delivery to the general community and to achieve its own stated corporate goals more readily.

Within the QPS, information technology has allowed police officers to perform their duties more efficiently, effectively and expeditiously. Advances in technology have facilitated new policing initiatives, such as intelligence-driven and problem-oriented policing. In years gone by, an investigator would have had to rely on a centralised service to provide information (i.e. the Information Bureau). The wait for a criminal-history check could be one day or several days, depending on the complexity of the inquiry and the workload of the Bureau. If further intelligence information was needed, the investigator would have to submit another request, which would go to the bottom of the list of tasks for the information processor at the Bureau. Consider the difference in efficiency in completing the same task today: an officer simply walks to a computer terminal and conducts the necessary search; if further information is required, it is only a keystroke away. The cost savings in terms of labour hours must be significant.

However, as became evident during this Inquiry (and was observed during previous CJC investigations), computerised information systems come with new and substantial risks to an organisation handling confidential and sensitive information. The misconduct observed in this Inquiry concerned improper access to, and/or release of, in-confidence material⁷ (e.g. personal details, criminal-charge history and traffic history) held on the computer systems, but this is not the only type of abuse that has been encountered with regard to the QPS computer systems.

The QPS has demonstrated a commitment to information security through the range of initiatives that it has implemented over several

years. It has established a framework for developing information policy, through which various information-security policies and procedures have been created. An Information Security Section (ISS) was created, which has both a proactive and a reactive role in implementing information security within the QPS. The Ethical Standards Command (ESC) was also established to promote ethical behaviour, discipline and professional practice through deterrence, education and systems improvement. The computerised information system has a feature that allows the transactions of computer users to be recorded.

However, it is the conclusion of this report that much more can be done to protect confidential information accessible by members of the QPS. As most of this information is now held within the computer systems, it is critical for the QPS to establish the most effective of security measures and policies to protect that information. Such protection is critical for a number of reasons:

- Much of the information accessible through the computer systems is personal and private information about individuals. It is important that individuals who provide information to the Government, or whose personal details are collected by the Government, are afforded the basic rights of privacy and confidentiality.
- If the Queensland Government were to introduce privacy legislation or adopt the Information Privacy Principles⁸ (discussed below), the QPS would not want to be in a position where costly changes would be necessary to modify work practices, policies and systems to avoid infringing the legislation.
- Improper release of information, as observed during this Inquiry, has the potential to compromise an individual's safety.
- If it were to be demonstrated that information improperly released from QPS computer systems resulted in injury or death, the Service may be liable and face considerable compensation costs.
- Another investigation or inquiry of this nature may reduce public confidence in the QPS and the trust accorded to it by other government agencies when sharing information with it.
- Information is a valuable commodity and consequently has a high value on the illicit market. The demand for illicit information is likely to become heavier as more information becomes available to a greater number of employees. Consequently, adequate security

systems need to be established to detect improper access conducted for personal reasons, on behalf of an unauthorised person or in exchange for a benefit.

- In compliance with legislative requirements,⁹ the QPS must develop an information-system strategic plan every year to provide for the needs of its clients and take into account relevant environmental factors. The QPS should consider the observations and outcomes of this Inquiry in the next planning cycle.

THE MARKET FOR INFORMATION AND THE BROKERS WHO FACILITATE INFORMATION EXCHANGE

Organisational information-security management is not the only way to respond to the problems revealed during this Inquiry. The exchange of information requires a giver and a receiver creating the supply and demand necessary for a lucrative market. In this Inquiry it was noted that the end-users who created the demand for information were mainly insurance companies, solicitors and leasing companies.

The end-users were generally concerned with locating a person whom they were unable to locate through conventional means. Often those being sought try to avoid being found and are fairly careful to ensure that publicly available records (e.g. electoral rolls) do not contain their address. In such cases, access to restricted government information, such as the motor-vehicle registration database or various police databases, is in high demand.

Private investigators and commercial agents act as intermediaries between the end-user and the supplier of information — in this Inquiry suppliers were members of the QPS. Closer examination of how the industry operates suggests that this market exists because the type of information sought is not accessible, under government policy, to the types of end-users identified in this Inquiry. One way to eliminate or at least reduce the illicit market may be by removing the current restrictions on access to this information. Like the debate over controlled access to dangerous drugs, this is not a straightforward issue. It is discussed in greater depth in chapter 7.

Considering the structure of the market leads to a matter of considerable concern to the CJC — that of regulation of those people who act as private investigators and commercial agents. Those individuals identified during this Inquiry who were either current or past private investigators

and/or commercial agents demonstrated a complete disregard for the law and did not hesitate to involve third parties, namely the subject police officers, in unlawfully obtaining confidential government information.

It was apparent to the CJC that inadequacies in the legislation regulating the two industries has contributed to the low standards of professionalism and integrity observed during this Inquiry. The CJC is concerned with the level and type of industry regulation that exists in Queensland because, before consideration can be given to providing these two industries with lawful access to restricted government information, their standards of professionalism and integrity must be significantly raised. This is the topic of chapter 8.

LEGISLATION TO PROTECT INFORMATION

It was inevitable that an Inquiry concerned with the release of the personal details of individuals would consider the adequacy of legislation designed to:

- protect the privacy of community members
- protect confidential government information
- prohibit unlawful access to and release of information.

Nationally and internationally, legislation protecting privacy and personal information is an increasing priority for governments. The significant events in the development of the privacy issue within Australia are shown in table 2.3 on page 12.

The privacy debate is not new in Queensland. The 1998 LCARC report, *Privacy in Queensland*, made 32 recommendations, including that:

- Queensland should introduce privacy legislation
- the legislation should include the IPPs relating to personal information collected and held by Queensland Government departments and agencies
- the IPPs should be modelled on those in s. 14 of the Commonwealth Act
- the legislation should provide for the establishment of a Privacy Committee or the office of Privacy Commissioner.

Table 2.3 — Events in the development of the privacy issue

YEAR	MILESTONE/EVENT
1966	The International Covenant on Civil and Political Rights is articulated and recognises the protection of privacy as a basic human right.
1975	NSW Government proclaims the <i>Privacy Committee Act 1975</i> .
1981	The OECD released <i>Guidelines on the Protection of Privacy and Transborder Flows of Personal Data</i> . This includes 12 recommendations, 8 of which are basic principles of national application. Australia being a member nation is subject to these principles. The guidelines recommend appropriate legal, administrative and other procedures for the protection of privacy and individual liberties with regard to personal data.
1981	The Council of Europe adopts a <i>Convention for the Protection of Individuals with Regard to the Automatic Processing of Data</i> .
1981	The Council of Europe recommends that its members adopt the OECD Guidelines by taking the principles into account when developing domestic legislation.
1983	The Australian Law Reform Commission releases the report <i>Privacy</i> , recommending adoption of 11 Information Privacy Principles (IPPs) — see appendix G — and the creation of the office of Privacy Commissioner.
1984	The Queensland Government passes the <i>Privacy Committee Act 1984</i> . An inaugural privacy committee is formed but, when its duty is completed, a subsequent committee is never formed.
1988	The Commonwealth proclaims the <i>Privacy Act 1988</i> . The Act includes, in section 14, the 11 IPPs (see appendix G) based on the OECD Guidelines, and provides standards for the collection, use, storage, transfer and exchange of personal information by Commonwealth agencies.
1989	The General Assembly of the United Nations adopts <i>Guidelines for the Regulation of Computerised Personal Data Files</i> .
1995	The <i>Convention for the Protection of Individuals with Regard to the Automatic Processing of Data</i> becomes binding on all adhering parties. Directive 95/46/EC of the European Parliament and the Council of the European Union requires all member states to pass laws that protect privacy rights to a consistent standard, promote the free flow of personal data within the European Union, and place restrictions on data being exported to other countries. Members given until 1998 to introduce such legislation.
1997	The European Union releases Information Sheet 3 on Directive 95/46/EC. On the matter of engaging in trade which involves the exchange of data with EU Member States, the Directive concludes that ‘As a country, Australia would be unlikely to be assessed as having an adequate standard of [privacy] protection in place. Apart from the Privacy Act, no other privacy legislation exists. However, a number of State governments are actively considering introducing data protection legislation’ (p. 3).
1998	The LCARC in Queensland releases its report <i>Privacy in Queensland</i> and recommends the establishment of privacy legislation and a Privacy Commissioner.
1998	The NSW Government proclaims the <i>Privacy and Personal Information Protection Act 1998</i> , which establishes a Privacy Commissioner.
2000	The South Australian Government announces a new Privacy Committee to advise the relevant Minister.
2000	On 12 April, the Commonwealth Attorney-General introduces the <i>Privacy Amendment (Private Sector) Bill 2000</i> into Federal Parliament.

Sources: Akindemowo (1999); LCARC (1998)

Note: This table does not include all events relating to the development of privacy issues within Australia.

Table 2.4 — Principles underpinning information management in the Queensland Public Sector

PRINCIPLE

1. Accountability	Each agency is accountable for all the information, in whatever medium and from whatever source, which it collects, processes, stores, and disseminates; only that information which is needed to fulfil its responsibilities to the government and the community should be collected and maintained.
2. Information Exchange	Each agency should ensure that government agencies (Federal, State and Local), the general public and the wider community, and the private sector, have reasonable right of access to government information, irrespective of the origin or location of that information.
3. Information Accessibility	Each agency should ensure that all of its key information, in whatever medium, is easily accessible by whoever is authorised, is properly defined and understood and, where appropriate, adheres to defined standards.
4. Compliance with Legal and Administrative Requirements	Each agency must comply with the legal and administrative requirements for managing information within the areas in which they operate.
5. Information Preservation	Each agency must ensure that information of enduring value is properly preserved in an accessible format for an appropriate time period.
6. Business Continuity	Each agency should ensure that it can continue to use and access its key information within the required business time frame, whatever the circumstances, including physical disruption.
7. Privacy and Confidentiality	Each agency should ensure the privacy and confidentiality of its information resource, and take all reasonable precautions to ensure that personal information (about individuals), commercial-in-confidence information (about organisations) or other sensitive information is not misused intentionally or unintentionally, either within the agency or when shared with external organisations.
8. Copyright and Other Intellectual Property	Each agency should ensure that copyright and other intellectual property issues are adequately addressed.

Source: Department of Communication and Information, Local Government and Planning, Queensland 1999

Before the release of the LCARC report (1998), the CJC was invited to make a submission on the issues paper on privacy that preceded the report. In that submission, the CJC expressed the view that the Commonwealth system of privacy protection embodied in the **Commonwealth Privacy Act 1988** was a useful basis from which a privacy-protection system could be created. The CJC also stated its support for the adoption of the IPPs within legislation and the appointment of a Privacy Commissioner.

Recently the Queensland Department of Communication and Information, Local

Government and Planning re-issued a number of standards relating to information security and information management.¹⁰ Information Standard 24 (1999) creates Government Policy that instructs all agencies to develop practices and policies that embrace the eight principles shown in table 2.4

The Department also released **Guidelines for the Management of Information within Government** to support Information Standard 24. In the section outlining Principle 7 on Privacy and Confidentiality (see Appendix H), the following statement is made:

The Queensland Government will be reviewing its position with regard to Information Privacy in the near future. However, each agency should be aware of the Information Privacy Principles contained in the Commonwealth Privacy Act 1998 ... and use them as guidelines where appropriate in the development of agency privacy policies. (p. 22)

The Government is clearly aware that community demand for some form of legislation to protect personal information and privacy is gaining momentum.

Given that this Inquiry was concerned with the management of personal information held by the Queensland Government (in particular by the QPS and Queensland Transport), and given the emerging trends within Australia and overseas, it is necessary for this report to make some comment on privacy legislation. This is the subject of chapter 9.

CONCLUSION

Information security is becoming an increasingly important priority for organisations within both the public and the private sector, nationally and internationally. The approach to information security has become much more strategic and broad. It is concerned with the protection of information from all types of threats. Organisations such as the OECD and Standards Australia have issued guidelines and standards on information security. Given the outcomes of this Inquiry, it is apparent that more can be done by the QPS to protect the confidential information that is accessible by its members. Protecting information should be a high priority for the QPS, as failure to do so may result in loss of confidence by stakeholders and other costly consequences (e.g. investigations and civil action by aggrieved individuals).

This Inquiry showed that there exists a market for information. The market is characterised by suppliers and buyers, with private investigators and commercial agents acting as the intermediaries. Issues such as industry regulation and public availability of government information are prominent when considering how the illicit market for information operates.

Legislation is another important element in protecting confidential government information from improper access and release. Laws to prohibit improper access and release of information are important, along with the privacy legislation. The privacy debate is not new in Queensland; there has been considerable debate on the issue as well as the release of a recent

report on privacy in Queensland by the LCARC (1998). The misconduct revealed by this Inquiry shows that privacy, as it relates to government-held information, must be given due consideration.

THE INVESTIGATION

The CJC conducted public hearings in respect of five distinct 'brackets' of evidence. Each bracket concerned a different complaint of alleged misuse of the QPS computer systems. This chapter gives a brief overview of the evidence gathered during each investigation and makes a number of observations based on this evidence.

The brackets concerned:

- police officers stationed at the Nerang Police Station who were accessing the QPS computer system and passing information on to a cleaner employed at the station, who also worked part-time as a private investigator and process-server
- a police officer stationed at the Inala Police Station who was using the QPS computer system to assist him in locating debtors on behalf of a debt-recovery agency for whom he was working
- a police officer who obtained the silent number of a woman from the QPS computer system and provided it to a man who she said had been stalking her over many years
- a police officer who was conducting hundreds of searches on the QPS computer system for personal reasons
- a police officer who was obtaining confidential information concerning a QPS investigation from the QPS computer system and providing the information to a person who was a potential suspect in that investigation.

The CJC cannot make findings of guilt but may refer particular matters to the appropriate prosecuting agency or the appropriate principal officer in a unit of public administration for disciplinary action. A number of reports have been forwarded to the Commissioner of Police for such disciplinary action as he considers necessary.

It is therefore inappropriate and unnecessary to descend into great detail in this report or to mention individuals by name. The purpose of this

chapter is to provide a backdrop against which a number of issues can be meaningfully discussed and recommendations made.

NERANG POLICE STATION

In August 1998, information was received by the CJC that a cleaner (N1), then employed by the Service at the Nerang Police Station, may have unlawfully obtained confidential information from the QPS and provided that information to a private investigator (N2), for whom he also worked.

On 6 October 1998, the CJC obtained documents said to relate to investigations undertaken by N2 in the course of his occupation as a private investigator. The particular documents concerned a two-year period from 1996 to 1998. The CJC was also handed invoices evidencing payments allegedly made by N2 to an informant identified by a code name that could be interpreted as N1's Christian name.

In general terms, the documents related to investigations of particular individuals — investigations that N2 was instructed by his clients to undertake on their behalf. The clients included solicitors, finance and insurance companies and others.

The CJC provided the Information Security Section (ISS) of the QPS with the names of those people whom N2 was investigating and asked that a search be conducted on the names with a view to determining whether any QPS officers had searched for them on the QPS computer systems. This analysis is known as a QueryMaster Inquiry.

As a result of the QueryMaster Inquiry, it was established that two officers in particular, Senior Constable N3 and Constable N4, had conducted a large number of searches on many of the names of those under investigation by N2. Both of these officers had been stationed at the Nerang Police Station.

The CJC's major concern was whether or not officers N3 and N4 were being paid for

unlawfully providing confidential QPS information to N1 (the cleaner), who in turn passed the information on to N2 (the private investigator).

Documents seized by the CJC

On 27 November 1998 search warrants were executed by officers of the CJC on the premises of N1 and N2. Files for the period 1995 to 1998 inclusive were seized from each address.

Like the documents that the CJC had obtained earlier, the documents seized by the CJC related to investigations into particular individuals that N2 was instructed by his clients to undertake on their behalf.

Some of the instructions were very blunt. Solicitors from a number of firms specifically asked N2 to find out whether certain individuals had criminal histories. Frequently the information that was provided by N2 to his clients could only have come from a police database.

The QueryMaster Inquiry

Further QueryMaster inquiries were conducted in respect of the file names. The CJC received advice from the ISS that 72 QPS officers conducted command queries on individuals who were named in the files. A number of these officers were immediately eliminated from the investigation when, for example, it could be demonstrated from other material that the individual was the subject of ongoing QPS inquiries and that the searches were performed for this reason.

Some of the worst examples of multiple improper searches were those by a Sergeant who conducted 269 searches on 59 individuals, a former officer who conducted 147 inquiries on 41 people, and a Senior Sergeant who conducted 95 inquiries on 30 people. Senior Constable N3 conducted 1777 inquiries on 291 individuals during this period.

Witnesses interviewed

After eliminating many of the 72 officers from the Inquiry, the CJC interviewed 52 officers, of whom 34 were stationed or had been stationed at Nerang. Some had since left the QPS. The officers from Nerang were responsible for 2741 queries on 564 individuals.

N1 (the cleaner) and N2 (the private investigator) were summoned to a closed hearing of the CJC.

During interviews with the officers, some admitted to providing information to N1.

However, a number did not, even when faced with persuasive evidence to the contrary. Consequently, the CJC harboured doubts that these officers were being truthful.

In addition, a number of those officers who denied passing on information offered explanations that were markedly similar. This suggested collusion on their part in an effort to frustrate the CJC's inquiries and to avoid punishment. This collusion is discussed later in this chapter.

The most significant matter to remain unresolved was whether N1 had ever paid police officers for the information they provided. No officer confessed to receiving any payment for doing so, and N1 denied paying any officer for information.

The public hearing

As explained in chapter 1 ('Introduction'), a decision was made by the Commission to hold a public hearing concerning the Nerang Police Station with a view to resolving some of these issues. In particular, it was expected that the hearing process, which requires officers to give evidence on oath, would lead those officers to reconsider their position and admit to the misconduct that was suggested by the evidence.

This expectation proved correct. All of those officers who were called to give evidence, and who had previously denied passing information to N1, admitted to doing so, and to lying during their interviews.

The evidence

N1 was summoned to the CJC's hearings. In giving evidence, N1 stated that he began working at the Nerang Police Station as a QPS employee in 1990. Before starting work there, he met a number of Queensland police. This occurred in two ways: firstly through N2, when he worked for him in the late 1980s, and secondly, when he (N1) was a police officer in the Northern Territory and in the South Australia Police. While working for the South Australia Police he was involved in investigations that took him to the Gold Coast, where he met a number of police with whom he renewed acquaintance after moving there in 1987.

At the same time as he was working for the QPS, N1 was also doing ad-hoc work for N2 and working for himself as a private investigator and process-server. He admitted obtaining information from police officers at the Nerang Police Station.

He told the CJC that some of the information he

obtained from police was used for his private investigation work and some was given to N2. When asked by Counsel Assisting how much he was paid for the information supplied by Nerang Police Officers, he said:

To the best of my recollection anything between 10 or 15 dollars for a licence or registration check and anything from 30 up to 40 or 50 dollars for more detailed or traffic or [criminal] charge information. (CJC unpub., p. 224)

He said that his main and most reliable source of information was Senior Constable N3. He could not say when he first got to know Senior Constable N3. During the closed hearing he said, in reference to N3, 'There might have been a period that nothing went on at all for the first few years.'

Senior Constable N3 was transferred to the Nerang Police Station on 18 March 1993. The earliest evidence of N3 providing information to N1 (the cleaner) was a search he conducted on 8 January 1995. However, it should be remembered that the CJC only seized documents for the period 1995 to 1998 inclusive.

N1 told the CJC that he obtained information about individuals primarily for the purpose of locating them. However, broader checks, such as checks on criminal-charge records, traffic histories and warrants, were occasionally conducted. This admission was corroborated by material seized by the CJC and by the admissions of a number of officers who were examined by the CJC.

N1 told the CJC he knew that the police were not authorised to provide the information to him. He wanted the fact that he obtained information from the police kept confidential. N1 also told the CJC that the Nerang Police Station was his principal source of information in the more difficult cases. N2 (the private investigator) also said that he knew that some of the information could have only come from the police and that it was illegal for police to provide information from the QPS computer systems.

When asked why he did not obtain the information through alternative sources, N1 stated 'Probably didn't think about it, and possibly the convenience, the way I was getting things, and the speed' (CJC unpub., p. 238). He later agreed with Counsel Assisting that he continued to seek information in this way because it was 'reliable, speedy and cheap' (CJC unpub., p. 238).

All of the police who gave evidence before the

CJC agreed that providing the information was unlawful. All denied being paid for providing the information.

Widespread practice at Nerang Police Station

The misconduct exposed by the CJC's investigation had persisted at the Nerang Police Station for some years and on a large scale. It ceased only because of the CJC's investigation. The practice seemed to be accepted and commonplace.

A number of examples illustrate the point:

- N1 told the CJC that no officer had ever refused his requests for information unless he or she was too busy at the time.
- No officer said that he or she was directed by a senior officer to conduct a search for N1.
- None of the officers made any attempt to satisfy themselves that N1 was genuine.
- No officers sighted any documents in N1's possession that could have supported or justified the requests for information.
- N3 told the CJC that 'it was the accepted thing [to conduct searches for N1] at the Nerang Station at the time' (CJC, unpub, p. 253). He also said 'I was never directed or never told but from other officers I was told that it's accepted that you could do it with the sanction of the senior officers' (CJC unpub. p. 263).
- Some officers spoke of witnessing N1 sitting in front of a QPS computer and scribbling down notes or passing pieces of paper to officers at a computer and those officers doing checks on the computer. On the evidence, it is likely that this was a frequent occurrence. Given his position at the Nerang Police Station, this should have attracted the attention of some of the staff to his behaviour.

Subjective test for disclosure of information

Although they knew it was unlawful, several officers said they saw no harm in the practice. Three examples will suffice to make the point:

Due to the circumstance, in that, I was of the belief that it was for a process [to assist N1 in serving court documents], basically I didn't see any harm in doing it. (CJC unpub., p. 86)

I was aware that it was wrong but I — under the circumstances I didn't think it was harmful in any way. (CJC unpub., p. 101)

I trusted him. I honestly didn't think it would do any harm if he was doing what I believed he was doing, to locate persons for whatever reasons it was, by me providing him with an address then he would get that done. That was the reason I gave him the information. (CJC unpub., pp. 143–44)

Comments such as these suggest that the officers applied a subjective test as to whether they should provide the information rather than abiding by the law and QPS policies.

The folly of such an approach was demonstrated during several brackets of evidence, including one instance when an officer from Nerang provided information to N1 that was used to locate a woman who, with her daughter, had fled from a violent relationship with her husband. She had even severed ties with her family to avoid her husband's attention.

Culture of acceptance at Nerang

The evidence heard during the Inquiry demonstrated an unwillingness by many officers to accept that the release of a citizen's private details is wrong and potentially harmful. For those officers, where their entrenched view conflicted with the law, it was their view that prevailed. The culture of acceptance included an unwillingness to question or report the conduct of police officers who provided information to the cleaner. The cleaner at Nerang and the other ex-police private investigator were able to exploit this opportunity.

The fact that the cleaner (N1) of the station was an ex-police officer was a significant factor for a number of Nerang officers. N3 said 'We regarded him [N1] as one of us, being ex-police there seems to be that tight-knit circle whether you're ex or whether you're current' (CJC unpub., p. 251). Another officer (N7) stated that one of the reasons he did the computer checks was that he knew that N1 was an ex-police officer from the South Australian Police 'who had an interest in his neighbourhood and what was going on at work' (CJC unpub., p. 97).

N1 himself stated that he managed to maintain goodwill with the Nerang police because of 'camaraderie between perhaps an ex-member of the force, present member, the general culture of things, same sort of talk' (CJC unpub., p. 229).

The CJC also heard evidence that information obtained from the QPS computer system had been provided by some Nerang police to two other private investigators, one of whom was an ex-QPS officer, and the other a former Australian

Federal Police officer.

It was this culture of acceptance that contributed to the involvement of so many officers in this unlawful practice for so long. Constable N5 said she knew that she was not entitled to give N1 the information but 'because [N1] was friendly with the other police there, I felt hard — it was hard for me to say no' (CJC unpub., p. 53).

Constable N4 was new to the Nerang station when he first provided information to N1. He gave three explanations for doing so: firstly, stupidity; secondly, he saw no harm in providing the information; thirdly, his fear of the consequences if he refused:

I suspected it was — seeing [N1's] popularity within the station — I suspected that if I didn't provide him with the checks he may have gone to some other person because I was new to the station at that time and he may have gone to the other members of the station and said, 'Well this [name of witness] is, maybe, a bit of a dog', or — I just felt — I just wanted to be accepted in the station and I felt that that may be — if I did the checks I might at least be talked to and I suspected that was my main reason. (CJC unpub., p. 122)

This officer lied to the CJC during his disciplinary interview, but during the public hearing admitted to providing information to N1. He said that he knew the names of other police who were doing computer checks for N1 but did not name them in the interview because he wanted to protect them.

Constable N4 was also advised by other officers to 'tough it out', meaning that he should deny involvement in this unlawful behaviour until the investigation was over. The following exchange occurred between Counsel Assisting and another officer, Senior Constable N6:

Counsel Assisting: Did you feel a need to comply out of a need to belong to the station and be accepted there; was that part of your motivation?

N6: Yes, but not in the sense that it was a police station, that I was a police officer — I would feel that that would apply to anywhere that I was going to be working ... to fit in with the run of things.

Counsel Assisting: Did it cross your mind in the early days that to refuse to comply might have branded you as some kind of misfit?

N6: Yes, and I would base that on certain things that I've seen in my service.

Counsel Assisting: And so to take that to its logical conclusion if you were to refuse N1's request you might be regarded by some as then being an officer not to be trusted?

N6: That is something that could, in fact, occur, yes.

Counsel Assisting: And presumably the irony of that position has struck you. You know you're not supposed to do it but you do it so that you can be trusted?

N6: That would be one way of looking at it certainly. (CJC unpub., pp. 154–55)

The evidence of these officers suggests that they felt compelled to participate in an unlawful practice because they feared being ostracised by their fellow officers if they did not.

Other evidence suggested collusion on the part of some officers in an effort to frustrate the CJC's inquiries and to avoid punishment. For example, in trying to explain how N1 may have come into possession of computer print-outs of searches that they had undertaken, several officers suggested that N1, being a cleaner, must have taken them from the waste-paper bins. Constable N4 agreed that the subject of print-outs was discussed with fellow officers from Nerang when it was decided to 'tough it out'.

Many officers stated that they were regularly supplied with information by N1 about possible criminal activity and that they would have conducted searches on people who were the subject of that information. It followed, so the argument went, that N1 was actually supplying information, perhaps even false information, about his clients, and this explained why their names coincided with searches by the officers.

The truth was that N1 provided officers with information from time to time but, with few exceptions, none of it was of any value. No-one considered that there was a fair trade of information between N1 and any officer. Another officer considered that N1 provided information to him so that the officer would later feel obliged to provide information in return. N1 denied this.

Constable N4 frankly admitted that the explanation concerning the provision of information by N1 was one that was to be commonly adopted by police during the CJC's investigation. The evidence was as follows:

Counsel Assisting: So did you get together especially to discuss this situation [the CJC investigation]?

N4: No, no, no. No, it just come up in

conversation — just in conversation.

Counsel Assisting: Okay. Have you ever been in that situation before, that in conversation you and your fellow officers had decided to take a joint line on anything like this?

N4: No, not really. It's just — no, there was no — how you went about doing it, you went about doing it.

Counsel Assisting: The question probably assumes something. Did you read the conversations with your fellow officers as a — as showing an intention to take a joint line?

N4: No, not really — not really. I could have gone out on a limb if I wanted to.

Counsel Assisting: But it was a discussion about toughing it out?

N4: Generally, yes.

Counsel Assisting: Okay?

N4: I suppose.

Counsel Assisting: And one of the aspects that you were untruthful about in the 5 August '99 interview, was that [N1] helped you out with information?

N4: That's correct. That was untruthful.

Counsel Assisting: Now that was one of the lines of defence, wasn't it?

N4: Yes. Yes.

Counsel Assisting: And so far as your personal experience is concerned, that just wasn't the case, [N1] never provided information to you?

N4: No.

Counsel Assisting: Right?

N4: No.

Counsel Assisting: And in the conversations with your fellow officers, was that suggested as a line that officers might take if they wished?

N4: Yes.

Counsel Assisting: And did that suggestion come from a particular officer?

N4: No. No, it came from generally everyone.

Counsel Assisting: And it was acknowledged by other officers that it would not be the truthful situation but that it seemed like a good explanation?

N4: Yes. (CJC unpub., p. 127)

Other officers who conceded that this explanation was false refused to concede that they gave the explanation because they were told to or because it was part of a common 'defence'.

Finally, no officer claimed to know that N1 was working for another person (N2). One officer maintained that he did not even turn his mind to the prospect that N1 was making money from what the police at Nerang were doing for him.

Summary of the evidence

The following points summarise the evidence:

- N1 admitted to obtaining information from officers at the Nerang Police Station concerning current addresses, criminal charge records, traffic histories and warrants over several years.
- N1 admitted to passing the information on to N2 for a fee that depended on the nature of the information.
- The practice was widespread and involved hundreds of computer inquiries by officers who admitted that they knew it was unlawful to do so.
- Both N1 and N2 admitted that they knew it was unlawful to obtain information in this way.
- N1 said that he used the police to obtain information because it was 'reliable, speedy and cheap'.
- The extent to which officers were told by other officers that the practice was permissible cannot be assessed with certainty. At the very least it would appear that the practice was so entrenched at Nerang that it was assumed by staff to be something that was condoned by senior officers.
- There is no evidence of payments being made by N1 to any officers for the information.
- No officers said that they knew that N1 was passing on information to N2.
- Some officers said that the fact that N1 was a former police officer played a significant part in officers' agreeing to provide the information to him. Other evidence disclosed that two other private investigators were supplied with information, both of whom were former police.
- Some officers said that they conducted the searches out of fear of the consequences from other officers if they refused.
- Once it became known that the CJC was conducting an investigation, there were conversations between police officers in which they discussed what stance they would take if questioned by the CJC.
- A number of police officers lied to CJC

investigators during disciplinary interviews, but at the public hearing admitted to their involvement in this matter, and to the fact that they had lied previously.

Outcomes of disciplinary proceedings

Twelve currently serving officers who were involved in the misconduct at Nerang station have been subject to the disciplinary process. Former members of the QPS who engaged in the misconduct cannot be subject to QPS disciplinary process.

To date, five serving members have been disciplined. The outcomes are as follows:

- two officers demoted from Senior Constable 2.1 to 1.1
- one officer demoted from Senior Sergeant 4.1 to Senior Constable 2.3
- one constable demoted from Constable 1.6 to Constable 1.1
- one officer demoted from Detective Sergeant 3.3 to Constable 1.6.

It has been indicated that each officer who was so disciplined will be seeking to have the demotion reviewed by the Misconduct Tribunal.

INALA POLICE STATION

This investigation concerned an allegation that a Senior Sergeant, In1, stationed at the Inala Police Station, was using the QPS computer system to locate debtors on behalf of a debt-collection agency.

Senior Sergeant In1 was sworn into the QPS in 1974. In 1993 he was promoted to Senior Sergeant at the Inala Police Station, and later, in 1999, was appointed as the officer in charge of the station.

Files were obtained from the collection agency by the CJC, and QueryMaster Inquiries were conducted in respect of the subject names found on the files. These resulted in a number of names being identified as the subject of searches by In1. Additional searches were conducted under the user-identification codes of six other officers at Inala.

In1 was interviewed by the CJC on 16 December 1999. At first he denied using the QPS computer to assist him in his business, but eventually he agreed that he had done so.

In1 was summoned to give evidence before the CJC. He told the CJC that, as well as working for the QPS, he worked as a sub-agent for a debt-

collection agency. Although he did some work for the agency in late 1998, the bulk of his work commenced in February 1999. This was when he was registered as a sub-agent for the agency.

As a sub-agent, he was given instructions by the agency, acting on behalf of various finance companies, to attend meetings in certain locations to discuss issues relating to a debtor's outstanding loan. It was often necessary to first locate the debtor. To do this, In1 would resort to a number of commercially available sources of information. Sometimes, however, these inquiries were unsuccessful. It was then that In1 would use the QPS computer at the Inala Police Station.

On occasions, In1 also made inquiries about people he could locate. He did this because, after speaking to them, he thought that something was not, to use his words, 'quite kosher and they were hiding something'. He cited one example where his suspicions were confirmed by the existence of warrants relating to the person.

The principal of the collection agency told the CJC that In1 was detailed an estimated 335 jobs during the period when he worked for his agency. He stated that, during the period 17 February 1999 to 8 December 1999, the subject officer was paid a total sum of \$10,039.40 by the agency. Of course, only some of these jobs were discharged with the aid of searches on the police computer. The CJC's inquiries suggest that he conducted searches on 22 people.

Of particular concern was the fact that searches on names connected to the collection agency's files were conducted under the computer-user identification codes of six other officers stationed at the Inala Police Station. All of the officers denied conducting these searches. In evidence, In1 admitted that he did the searches and that he had never asked another officer to do them for him. He said that he must have used a computer that was left open and unattended.

In1 also admitted that he knew that what he did was contrary to QPS directions:

Chairperson: Senior Sergeant, did you understand at the time that you carried out these checks that to do so was contrary to the directions and procedures for the use of the QPS computer system?

In1: I did, sir, yes, and I admitted that, too. It flashes up on the screen every time you book on [referring to computer security warning screen].

Even though he knew it was wrong to do so, he

continued to do the checks:

Chairperson: Why did you proceed notwithstanding that?

In1: I suppose a bit of professional pride. I try to do everything that I do whether it be in my police work to the best of my ability and a bit of stubbornness about not letting things actually beat you. And I've never been one who likes to see a crook or somebody get away. I always like to pursue it to the best of my ability. I realise it was an error and I admitted it.

Chairperson: Now that overrode any commitment or pride you had in relation to acting properly as a police officer?

In1: I've had many discussions with my wife and a few other people about it and I have — I can't put my finger on any particular reason why I did it. It's — human nature is not as strong as you would like to think it would be. I always thought I had a very good and very strong sense of ethic and code but it's been tested and been proven and in all fairness to this Commission it's been in the back of my mind for many months even before they even started so it's something I chastised myself about on a regular basis and it was just a weakness and I've accepted that and I'm prepared to accept whatever happens from now on. (CJC unpub., pp. 528–29)

In1 was still conducting inquiries on the QPS computer in respect of the agency's work as late as November 1999. On 16 December 1999 he was interviewed by the CJC.

Outcome of disciplinary proceedings

This officer has recently resigned from the QPS. The resignation has been accepted and consequently this individual cannot be subject to QPS disciplinary process.

FORTITUDE VALLEY POLICE STATION

This investigation concerned an allegation that a Senior Constable (FV1) stationed at Fortitude Valley obtained the silent number and address of a woman (FV2) from the QPS computer system and provided it to a man (FV3) who she said had been stalking her over many years.

In September 1999, FV2 told the CJC that a man, FV3, whom she had been avoiding for many years because of his unwanted attention towards her, had contacted her on a silent number. FV2's husband contacted FV3 and asked him how he had obtained the telephone number. Eventually, FV3 told him that he had a very close friend who was a police officer in the Valley who had looked up their details and given him the phone number.

A QueryMaster Inquiry conducted on the QPS computer resulted in a number of police officers being suspected of conducting searches in connection with this case. All but one of the officers were eliminated¹¹ from the Inquiry by CJC investigators. The remaining officer, Senior Constable FV1 of the Fortitude Valley Police Station, was interviewed on several occasions by the CJC. During the first interview he told the CJC that he knew FV3, as he (FV3) worked in a café in the Valley and had served him on occasion. FV3 asked him to find out whether FV2, whom he described as his ex-girlfriend, had taken out a domestic violence order (DVO), as he (FV3) was concerned for her safety.

FV1 admitted conducting all of the checks identified by the QueryMaster Inquiry. However, he maintained that he merely confirmed the existence of the DVO to FV3. He said that he did not give out FV2's address or telephone number to FV3.

Subsequently, further audits revealed that, one hour after his initial checks, FV1 conducted other computer checks that would have given him access to FV2's silent telephone number. He was interviewed again but denied giving FV2's silent number to FV3. On five occasions during his two interviews, FV1 denied giving the telephone number to FV3.

FV1 was summoned to the CJC's hearing. Once there, he admitted that FV3 had asked him for FV2's telephone number, as a result of which he conducted the computer search, wrote down FV2's silent number on a piece of paper, and handed it to FV3. FV1 said:

I understand at the time that it was improper for me to provide that phone number to [FV3] but I was acting in good faith and I believe that the details he gave me were correct and that he was acting in the best interests of that other person. (CJC unpub., pp. 179–80)

When asked why he was untruthful during the two interviews with CJC investigators, he replied:

FV1: Because I knew my actions were improper and the reason that I did give that phone number to him wouldn't have satisfied the investigators.

Chairperson: Why did you understand that to be? Why?

FV1: Because I just knew that — providing that sort of detail is just improper under the legislation I work under. (CJC unpub., p. 180)

FV1 denied receiving any benefit from FV3 for providing the information. FV3 confirmed this.

FV1 maintained that he would not have undertaken these inquiries for just anyone, but he trusted FV3.

Outcome of disciplinary proceedings

This officer was disciplined and was demoted from Senior Constable 2.2 to Senior Constable 2.1.

NORTH QUEENSLAND POLICE STATION

This matter concerned an allegation that a Constable of Police, NQ1, stationed at a North Queensland Police Station, conducted hundreds of searches on the QPS computer system for personal reasons.

Constable NQ1 was sworn into the QPS in May 1999 and was assigned to general duties. His supervisor reported that, in the period 4 June 1999 to 18 August 1999, Constable NQ1 conducted 6900 inquiries on the QPS computer. Of those, it was suspected that at least 300 were not connected with official duties.

Constable NQ1 was interviewed by CJC investigators and later summoned to the public hearing. He maintained that the majority of the computer checks were legitimate. However, as there is no requirement for officers to record the reason for their searches, this could not be tested by the CJC.

Constable NQ1 was questioned by Counsel Assisting the CJC about a number of the computer inquiries he conducted. Some of these inquiries and the reasons he gave for conducting them are listed in table 3.1 on page 23.

As stated above, NQ1 was sworn into the QPS in May 1999. During his training, the Constable completed an assignment in which he commented upon the effect of s. 10.1 of the PSAA, which concerns improper access to QPS information. He wrote:

This section is probably the most pertinent to all recruits and first year constables at this stage of training. This section outlines that police are privileged to access information of a confidential nature. It also states that this information only be used for official purposes. The Service states that there is no excuse for a policeman to betray the public trust by making unauthorised, improper or unlawful searches. Examples include running a check on rego belonging to a good-looking nurse, or finding out whether a potential girlfriend has got any history. Failure to comply with this Act will result in disciplinary or criminal proceedings. This type of breach is

Table 3.1 — Reasons given for conducting improper searches on QPS computer systems

TYPE OF SEARCH PERFORMED	REASON FOR CONDUCTING THE SEARCH
Search on woman's name	The subject of the searches was a female acquaintance and the searches were conducted out of curiosity.
Search on his sister's name	Familiarising himself with the QPS computer system.
Search on woman's name	The Constable had met the woman on one occasion and was conducting the check to see whether she was 'clean', that is, without a criminal record, before he had anything more to do with her.
Search on woman's name	This woman lived in the same street as the Constable and he wanted to know whether he should associate with her.
Search on woman's name	This woman attended university with the Constable and he did the check out of curiosity.
Search on woman's name	This woman attended school with the Constable but now resided interstate. He did not have experience with the National Exchange of Police Information database and used this check as a training exercise.
Checks on Domestic Violence Index in respect of his home town (where his parents still resided)	Curious as to how the index worked.
Search on government vehicles that were for sale	The Constable was planning to buy a vehicle, and the checks were conducted in preparation for the purchase. He later bought one of the cars on which he conducted a search.

considered to be misconduct by the Service and will be dealt with accordingly. (CJC unpub., p. 619)

NQ1 was clearly trained and educated in the proper use of the QPS computer systems. Nevertheless, within six months of having received that training, NQ1 was conducting hundreds of improper and unauthorised checks on the QPS computer systems. For NQ1, the QPS training and education were an inadequate deterrent. Even when his supervisor expressed concern about the number of transactions he had performed, NQ1 continued to use the computer for personal reasons. The difference between what he knew to be the position at law and his actual practice is obvious.

Outcome of disciplinary proceedings

This officer was disciplined and fined \$450.

SOUTHPORT POLICE STATION

This matter concerned an allegation that a Constable of Police (S1) stationed at the Southport Police Station obtained confidential information about a QPS investigation from the QPS computer systems and provided the information to a person (S4) who was a potential suspect.

First computer check

On 9 November 1998, Constable S1 conducted a search on the registration number of a motorbike that he discovered was registered to S2. He then conducted searches on S2 to determine whether he had ever been charged with any criminal offences.

Motorcycle stolen

At 3.30 p.m. on 8 January 1999, S2 reported to the police that two armed men had come to his home at 1 p.m. that day and demanded his motorbike. They threatened to shoot S2 or 'kneecap' him if he did not comply with their demand. While they were there, another man

arrived at the house in a utility towing a horse float. The bike was loaded into the horse float and taken away.

As a result of the complaint, a criminal-offence report was generated on the QPS computer systems and a number, known as a Crime Reporting Information System for Police (CRISP) report number, was allocated.

Ownership of the bike had been the subject of a dispute between S2 and a woman, S3. She was therefore nominated in the CRISP report as a suspect, along with the two unidentified males who removed the bike (there should have been a third unidentified suspect, namely the driver of the utility).

Second computer check

At 29 minutes after midnight on 9 January 1999 a telephone call was made by S4 to the Southport Police Station. Constable S1 was on duty at the time. Computer audit trails show that, four minutes after the call was received at the station, Constable S1's user ID code was used to access the CRISP report that concerned the complaint by S2. An inquiry about the motorcycle was also conducted on the QPS computer systems.

The telephone call from S4 to the Southport Police Station lasted a little over 17 minutes. This shows that all the checks performed with regard to the CRISP report number and the motorcycle occurred during this telephone call.

Complaint lodged with the CJC

On the afternoon of 9 January 1999 one of the detectives who was assigned to the investigation discovered that, earlier that day, Constable S1 had conducted vehicle searches on the stolen motorcycle. He spoke to Constable S1, who told him that he had conducted the searches for a friend, S4. According to Constable S1, the bike belonged to a female friend of S4 and she could not get it back from S2. Constable S1 stated that he did a check on the motorcycle to see how it was listed.

The investigating detective asked Constable S1 to have S4 contact him by telephone. S4 subsequently telephoned the detective and during the call said:

When we first heard that on this crime report thing [the CRISP report], that he made these statements about guns used and this and that — what amazed, you know, the bloke's obviously — is just grasping at straws. (CJC unpub., p. 327)

Later in the conversation S4 stated:

His record, I found out about his record and all sorts of things and I thought it doesn't look like he's capable of assault or anything like that. (CJC unpub., p. 327)

The investigating detective lodged a complaint with the CJC, as it appeared that S4 was in possession of confidential information that could only have come from the QPS computer systems.

S4 admits to involvement in the offence

A QPS officer with twenty years' experience was assigned to the investigation. He interviewed S4, who admitted that he had arranged for the motorcycle to be picked up from S2's home and brought back to S4's place of work. S4 denied that Constable S1 or any other officer had given him information about the QPS investigation.

Public hearing of the CJC

S4 gave evidence before the public hearing of the CJC on 24 February 2000. During the hearing, S4 stated that in late 1998 he obtained advice from Constable S1 about what S3 should do to recover the bike. He was advised that S3 should lodge a complaint with the police. S4 stated that some weeks before the motorcycle was taken from S2, he asked Constable S1 to conduct a registration search on the motorcycle for him.

S4 maintained that he was provided with details of the alleged theft, including the allegation of a firearm being produced, as a result of information he received from S3. He also said that he obtained information about S2's criminal history from S3. When questioned further as to whether Constable S1 provided him with details of S2's criminal history, S4 stated that Constable S1 may have disclosed such details to him.

S4 stated that he could not remember if he spoke to Constable S1 on the morning of 9 January 1999, or, if he did, what their conversation was about.

Evidence of the Constable

While giving evidence at the CJC hearing, Constable S1 said that he told S4 to advise S3 to make a complaint to the police about the motorbike. Constable S1 stated that he had checked S2's criminal record but he could not remember whether or not he did so at S4's request. He said that S4 was worried about S3 because she told him that S2 had been violent towards her. He recalled telling S4 that it did not appear (from his criminal record) that S2 was a 'bad bastard'. He said that he would have

described S2 to S4 in general terms only and would not have gone into details of his criminal history.

Constable S1 told the CJC that he could not recall how or when he first learnt of the theft of the bike. He confirmed that he spoke to S4 on the morning of 9 January 1999 but he could not say why S4 rang him at that hour. He could not say whether S4 told him about the alleged theft or whether he already knew by that time.

Constable S1 stated that he did the checks on the computer that morning because he knew something about the history of the matter and did not know how much of that the investigating detectives knew. He said, 'So I wanted to get to the bottom of it pretty quick.' He could remember saying to S4 during the telephone call, 'What's happened? Supposedly someone's gone around there with guns and balaclavas and got the bike.' He remembered asking S4 what was going on. He recalled mentioning someone being knee-capped. Beyond these details, he had little recollection of the 17-minute conversation that occurred at 29 minutes after midnight on 9 January 1999.

Constable S1 stated that one of the investigating detectives rang him at home after he completed his shift and asked him to arrange for S4 to ring the investigator. The detective provided him with the CRISP number, but he could not remember whether the detective gave him the CRISP number or if he asked him for it.

He said that he spoke to S4 later that day and gave him the CRISP number so that he could quote it to the investigator. In this way, the investigating detective would know what S4 was talking about without having to go through all of the facts of the matter first.

According to Constable S1, it never occurred to him that S4 may have played some part in taking the bike. In short, Constable S1 denied acting improperly.

It is inappropriate for the CJC to draw any conclusions on the evidence in this report. What can be said is that the investigation of this serious allegation would have been materially assisted had there been a requirement that the subject officer record his reason for accessing the QPS computer on 9 November 1998 and 9 January 1999.

Outcome of disciplinary proceedings

This matter was heard before the Deputy Commissioner, who, after due consideration of all of the facts, found that the officer was liable to

disciplinary action for improper access to, and release of, confidential information from the QPS computer systems. The Deputy Commissioner demoted this officer from Constable 1.6 to 1.1.

The officer has appealed to the Misconduct Tribunal against the severity of the penalty.

CONCLUSION

During this Inquiry the CJC heard evidence of:

- unlawful access to the QPS computer systems by members of the QPS
- unlawful release of confidential information from the QPS computer systems by members of the QPS
- police officers from the ranks of Constable through to Senior Sergeant being involved in the suspected misconduct
- investigations concerning officers from a variety of city and regional stations
- police officers admitting to blatantly lying to superior officers during disciplinary interviews
- police officers admitting that they knew they were breaching QPS policies but did so regardless
- an unwillingness among staff at the Nerang Police Station to question or report wrongdoing by police officers
- collusion between some officers before being interviewed by CJC investigators
- particular officers advising other subject officers to 'tough out' the CJC investigation.

Together with the outcomes from previous investigations, there is sufficient evidence to suggest that information systems are being readily abused and that new information-security measures are needed to counter the abuse. This is the topic of chapters 5 and 6.

The CJC considers that a firm disciplinary approach must be taken to proven misconduct of this nature. This will serve as a deterrent and send a message to other members that this type of behaviour will not be tolerated. The QPS has already taken disciplinary action against the majority of the subject officers who appeared before the Public Inquiry, most of whom have been demoted.

THE NATURE OF THE MISCONDUCT

The CJC has allocated significant resources to this investigation and report because it considers that improper access to, and release of, confidential information from the QPS computer systems is a serious and possibly prevalent form of misconduct, and therefore needs urgent consideration from a prevention and risk-reduction perspective. The CJC has considered a number of issues before deciding, on this occasion, to release a public report.

The purpose of this chapter is to outline those issues that the CJC considers to be important and, where appropriate, to quote from the submissions and comments of the stakeholders. The first section of the chapter describes the CJC experience of investigating this type of misconduct. The next section outlines the frustrations encountered when investigating complaints of improper access to and/or release of confidential information.

The CJC considered the following issues concerning the nature of this type of misconduct:

- the motivation of subject officers in committing this type of misconduct
- complaints statistics as an indicator of prevalence
- the potential for abuse
- the marketability and value of confidential information
- stakeholder concern for the protection of confidential information.

Each is discussed in turn and, where relevant, the views and submissions of stakeholders on each issue are outlined. The final section of the chapter discusses the funding issues that the QPS asked the CJC to consider when developing its recommendations.

PREVIOUS CJC EXPERIENCE

The kind of misconduct revealed during this Inquiry has been the subject of investigation by the CJC over many years. In 1994 Mr Rob O'Regan QC, the then Chairperson of the CJC, wrote to the Commissioner of Police about his concerns:

The Commission has written to the Police Service on a number of occasions expressing its concern about the problem [misuse of confidential information] and I readily acknowledge that you and your predecessor have taken steps aimed at addressing the issue. I respectfully suggest however that the continuing high number of allegations of misuse of confidential information indicate that further remedial action is required.

Later that year, Mr O'Regan wrote again, expressing the concerns of the CJC:

You would be aware that some alarming circumstances have been uncovered through the investigation of complaints made to the Commission, including identification of officers in sensitive positions providing information to private investigators and commercial agents.

Two years later the CJC was to commence a major covert operation that ultimately led to a Public Inquiry (Police and Drugs) in 1997. During that Inquiry, evidence was heard that members of the QPS improperly accessed and/or released confidential information from the QPS computer systems. In the report of that Inquiry (CJC 1997a), the following example from Operation Caesar II was documented:

On the evening of 16 June 1996, GC14 [a CJC covert agent] attended a meeting with a serving police officer and the former officer C, and an apparently corrupt arrangement was entered into. On the next morning, 17 June 1996, the police officer concerned, at 1023 hours, conducted computer checks on GC14. At 1132 hours, a public servant conducted checks on

GC14, and at 1231 hours, another police officer employed as a District Intelligence Officer conducted further checks on GC14. There is no basis for any valid belief that at that time police had any interest in GC14 for law enforcement purposes. He was apparently not known to police, nor was there any interest in him as a person involved in unlawful activities. The last two checks made in respect of GC14 were clearly made on behalf of serving police. Those persons who made the checks were, not surprisingly, unable or unwilling to say on whose behalf the checks were made or for what purposes. (CJC 1997a, pp. 59–60)

The former police officer and the serving police officer referred to in the above quote, who entered into the corrupt arrangement, were convicted of corruption and perjury charges as a result of Operation Caesar II and are currently serving terms of imprisonment.

The CJC's investigations in Operation Caesar II led to a broader inquiry into the extent to which a serving police officer assisted the former police officer, who was a private investigator, by providing him with confidential information that the serving police officer had obtained from the QPS computer systems. The serving officer was later charged before the Misconduct Tribunal with six charges of official misconduct, the first five of which related to unlawfully accessing and disclosing confidential QPS information to the former police officer. These charges concerned 90 searches on 7 individuals. The sixth charge concerned unlawfully accessing the QPS computer systems on 155 occasions in respect of 21 people. The officer pleaded guilty to the charges.

During the course of submissions on his behalf, the serving officer's Counsel stated that, although it was clearly wrong for a police officer to disclose confidential information without authority, such wrongful disclosure 'happens and it happens on a very regular basis'. Of course the CJC is mindful that these submissions were made by Counsel acting on the instructions from an officer facing serious disciplinary charges.

Another example from the Police and Drugs Inquiry (CJC 1997a) was observed during Operation Lime:

In the course of the execution of their [the police under investigation] illegal plan, they observed certain vehicles which they believed may have been surveillance vehicles. Their first thought was that their target for the robbery may also have been the subject of surveillance by an undisclosed law enforcement agency. In

fact, they were the subject of surveillance by Commission staff. Both police officers at the time were not on duty. At 2110 hours, a female employee at the police station where the two police officers then were, checked the details of one of the surveillance vehicles and, between 2120 hours and 2156 hours, one of the officers also checked the details of the same vehicles. Later, at 2305 hours, the woman made checks on another of the surveillance vehicles. ... Two days later, on 26 June 1997, three further checks on surveillance vehicles were made by one of the police officers and by civilian employees.

It is clear that these police officers, even in the course of executing their criminal plan and for the purpose of assisting and facilitating it, made computer checks on vehicles including surveillance vehicles. They also recruited innocent civilian staff for the same reason. Their intention was clear, namely to be able to satisfy themselves whether their unlawful activities may have been compromised by the occupants of the vehicles which they observed in the vicinity. For this purpose, they used their capacity to access the official information. The information was used not only for a private purpose but for a corrupt private purpose. (CJC 1997a, pp. 62–63)

The two police officers were later convicted of conspiracy offences and sentenced to terms of imprisonment.

THE DIFFICULTIES FRUSTRATING PRODUCTIVE INVESTIGATION

It was fortunate that, for the investigations outlined above, the CJC was able to demonstrate the improper and/or unlawful actions of the subject officers. Often the CJC is simply not able to investigate the matters productively. Although computer audit trails are maintained by the QPS, without a mandatory requirement for members of the QPS to account for their transactions, suspect members are able to hide behind claims that they:

- 'cannot recall' why they performed the transaction
- could have performed the transaction on someone else's behalf but have no recollection as to who that person might have been
- often leave the computer terminal open and it must have been someone else who used their user ID.

As outlined in the above section, in both Operation Caesar II and Operation Lime, not only did the officers who were the subject of the investigation misuse the QPS computer systems, but they were able, without explanation, to ask other QPS members to conduct computer checks on their behalf.

For many complaints the CJC and ESC (Ethical Standards Command) simply do not have a starting point to commence an investigation. The exception is where there is additional evidence or information to assist in the investigation. For example, in the Nerang matter the files that were seized from the private investigator were able to be compared with the QPS computer audit trails. As a result the connection became obvious and provided the basis upon which this investigation progressed; the private investigator often recorded personal and confidential details about individuals — details that could only have come from the QPS computer systems — and the QPS audit trails showed that certain members had accessed the records of these individuals in the days or weeks before the private investigator recorded them. Even with this compelling evidence, the CJC had to use a public hearing to get to the truth of the matters; the majority of subject officers called before the public hearings admitted that they had lied to CJC investigators during their earlier interviews.

Investigations into this type of misconduct have been extremely costly for both the QPS and the CJC. They are often protracted because of the need to conduct numerous interviews in concert with private and public hearings to get to the truth of the matters. This makes it important to identify areas where modifications and improvements in policy and practice can be made to minimise the opportunities for the abuses to occur, and to ensure that there are effective mechanisms to deter employees who may be tempted to engage in such conduct. In addition, methods can be developed to assist in the investigation of allegations. The priority for both the QPS and the CJC must be to minimise the need to conduct such an Inquiry again. The implementation of the recommendations of this report will go towards achieving that objective.

THE MOTIVATION TO COMMIT THIS TYPE OF MISCONDUCT

As is evident from the description of previous CJC investigations and of Project Piper, the motivation for members to engage in this type of misconduct varied. The people convicted as a result of the Police and Drugs Inquiry (CJC 1997a) are proven examples of corrupt police accessing the QPS computer systems to further their criminal activities.

The stated motivation of many subject officers identified during Project Piper did not include any obviously corrupt intent. Many stated in evidence that they knew, either at the time or in hindsight, that their actions were against QPS policy and were unlawful, but nevertheless felt justified in deviating from policy and the law. They all claimed to believe that, at the time when they conducted the computer checks and/or provided information, they had a valid reason for their activities. Examples of the reasons given to justify these actions were:

- the person to whom the information was being supplied was an ex-police officer and could be afforded a higher level of trust than was normally the case
- there was a common goal shared by the person requesting the information and the subject officers, as the person in question was often performing tasks (e.g. serving court documents) in relation to individuals who were avoiding their lawful obligations
- the person requesting the information, in the opinion of the subject officer(s), was of good character and had good intentions
- to conduct a probity check on an acquaintance.

While the motivation and reasons for committing this type of misconduct may vary, it is still fundamentally an invasion of privacy and a breach of the law and the trust of those individuals whose personal details are being improperly accessed and/or released. It is also worth noting that the process of abuse (i.e. using QPS mainframe/corporate computer systems) and the difficulties encountered when attempting to detect and investigate these types of matters are the same regardless of the motivation of the subject members. This is one of several issues that were considered by the CJC when preparing this report.

COMPLAINTS STATISTICS AS AN INDICATOR OF PREVALENCE

For some forms of misconduct, the CJC and the QPS rely on complaints and complaint substantiation statistics for an approximate estimation of the extent of the problem. In its submission to this Inquiry, the QPS observed that:

Service records indicate that since 1 July 1992 approximately 100 complaints concerning 120 allegations of misuse or improper access of information have occurred each year. Approximately 22 allegations are substantiated each year, with an average of 2.4 allegations each year serious enough to warrant a

disciplinary sanction above that of a caution or reprimand. (QPS submission 2000, p. 8)

According to the Police Service statistics, serious instances of misuse of confidential information occur at a rate of about 2.6 per year, or five every two years.

That has to be considered in the context that the database of the Police Service is accessed approximately 120 million times per year, so we are looking at an absolutely tiny percentage ... (CJC unpub., p. 905)

The Service indicates there have been relatively few complaints of unauthorised access or disclosure and, in part, relies on this to support the conclusion that this is not a 'major' problem. However, for this particular type of misconduct these types of statistics are limited in their usefulness in estimating how prevalent the problem may be.

As stated in evidence by Dr Brereton, Director of the Research and Prevention Division of the CJC, 'victims' are often not aware that information about them has been improperly accessed and/or released, and so are not in a position to make a complaint:

For some types of complaints such as some types of police misbehaviour such as assaulting suspects you have an aggrieved complainant who in many cases will take some action. In the case of information breaches, often the person who is disadvantaged by the release of the information may not be aware of that so you don't, in a normal sense, have a victim. (CJC unpub., p. 639)

Despite the fact that this Inquiry showed hundreds of instances of improper access and/or release of information about hundreds of people by members of the QPS, only one matter was detected because of a complaint lodged by the 'victim'. In this instance, the complainant was able to make a complaint because she was told that her silent phone number had been released by a police officer; in the majority of cases the 'victim' is not aware of what has occurred. This example reinforces the view that, for this type of misconduct, the complaints process should not be relied upon as a comprehensive system of detection or a precise measure of prevalence.

In this investigation, the initial information about the Nerang police station was received on 21 August 1998. Further investigations revealed suspicious computer transactions dating back to January 1995, which indicates that this type of misconduct has been occurring for many years without detection. It is quite likely that, had CJC

intelligence information not pointed to the problem, this behaviour would still be occurring today. Given that the capacity for current systems to detect this type of misconduct is low, the only accurate conclusion that can be drawn is that the prevalence of this misconduct is largely unknown.

Another problem with simply counting complaints is that those numbers tend to under-represent the number of discrete instances of misconduct. For example, an assault complaint generally relates to one discrete act of assault (e.g. the police officer is accused of using excessive force when arresting a person). However, a single complaint of information misuse may cover only one instance involving one person, as in the Fortitude Valley matter, or it may involve multiple officers with regard to hundreds of discrete acts of misconduct. In this Inquiry, on the basis of one single complaint,¹² 34 former/current members of the QPS came under suspicion for improperly accessing and releasing information. Of these, there is persuasive evidence of 17 former and current police officers being involved in hundreds of instances of unlawful access to, and disclosure of, confidential QPS information. Twelve serving police officers from the Nerang Police Station have been subject to, or are to be subject to, disciplinary actions.

The unreliability of complaints numbers as an indicator of prevalence is also demonstrated by the substantial increase in complaints of this nature since the Inquiry was announced on 27 January 2000. Since that time, the CJC has received approximately 170 complaints¹³ that make one or more allegations of inappropriate access to and/or release of confidential information by a member of the QPS. This number, covering an eight-month period, is substantially higher than the QPS yearly average of 100. Of the complaints that have been made since the announcement of this Inquiry, 124 have come from the public, indicating that the increases may be due to increased community awareness of the issue and of the CJC's responsibility for investigating such complaints.

Substantiation rates are also unreliable as an indicator of how prevalent or serious this type of misconduct is. Not only is this type of misconduct difficult to detect (as discussed above), it is also very difficult to investigate productively. It is not surprising, then, that substantiation rates are low. Therefore substantiation statistics, like complaints statistics, should not be relied upon as an accurate estimate of the extent of the problem.

Given the above points, it is highly probable that

complaints rates and substantiation rates significantly under-represent the true prevalence of this type of misconduct.

THE POTENTIAL FOR ABUSE

When considering whether prevention and risk-reduction measures are the best response to this type of misconduct, it is a useful exercise, particularly from a risk-management perspective, to consider the potential for abuse to occur.

With regard to this particular Inquiry, the QPS concluded that 'whilst the Service is naturally concerned by the instances of unauthorised disclosure, the magnitude of the problem should not be exaggerated' (QPS submission 2000, p. 25). In support of this conclusion, the QPS commented that:

The few identified instances of unauthorised access or disclosure ... appear to be isolated, both geographically and in time, and in terms of the personnel involved, negating the existence of any systemic problem. (QPS submission 2000, p. 25)

The QPS representative at the close of public hearing, Mr Morris QC, also submitted the following:

I'd like to finish, if I may, Mr Commissioner, by identifying what I'll call the fundamentals, fundamentals that in the submission of the Police Service emerge from the evidence that has been received in the course of this inquiry and the submissions that have been advanced from a variety of sources. The first fundamental is that this is not a major problem. Any misuse of confidential information, of course, is a problem, but in the scale of things, this isn't a problem of huge magnitude. (CJC unpub., p. 905)

With regard to the current Inquiry, it was demonstrated that a number of officers, from different areas of the Service (Fortitude Valley, Inala, Northern Queensland, Nerang and Southport), were willing to improperly access and/or release confidential information to an unauthorised person. It was often personal information about individuals that was disclosed, seriously compromising their right to privacy and, in those cases where they knew of it, their confidence in the ability of the QPS to protect this information effectively.

Of particular concern to the CJC was the misconduct by so many officers at the Nerang Police Station. Many of those officers were transferred to Nerang during the relevant period and quickly became involved in the unlawful

activities. This is particularly worrying because police officers are sworn to enforce the law and are obligated under the PSAA to report suspected misconduct. The behaviour only ceased with the commencement of the CJC investigation.

The QPS has submitted that the observations of the Nerang matter may be the result of 'group think' specific to that location. However, an important aspect of what occurred in Nerang was that, despite officers coming into Nerang from other stations, it would appear that none challenged or even questioned the practice that had become entrenched at Nerang. Such behaviour suggests that the culture evident at Nerang was not unique to that location.

In many of the cases investigated by the CJC, the evidence established that there was a reluctance among officers to accept that the release of a citizen's private details is wrong and potentially harmful. This may reflect a culture that places little significance on protecting this type of information, notwithstanding the legal requirements. Within such a culture, the release of information to process servers and private investigators may be viewed as desirable because it advances broad law-enforcement objectives. There is a risk that such thinking may exist or could develop in other parts of the Service.

Furthermore, integral to the misconduct that occurred at the Nerang Police Station was a willingness by officers to accept without question the unlawful conduct of other police. The cleaner at the Nerang Police Station and other ex-police private investigators were able to exploit this opportunity to access information unlawfully. This sense of camaraderie among police and former police is not unique to Nerang. The prevalence of private investigators who are former police officers throughout the State means that the possibility that this culture of acceptance is more widespread must be taken seriously. The concern of the CJC is that if this can occur in one police station it could equally occur in another police station. It is necessary to further develop QPS systems and controls to ensure that the risk of this practice developing in other police stations is minimised.

The other critical issue noted during this and other CJC investigations is the ease with which an individual officer can misuse the QPS computer systems without fear of detection. This conclusion is also consistent with the perceptions of junior police officers regarding detection. As discussed on page 65, when compared with other forms of misconduct, this type of misconduct is seen by junior police officers as among the ones that are least likely to be detected.

In addition, it is worthwhile noting that, despite the media attention generated during this Inquiry, another CJC investigation being conducted at the time of the Inquiry found police officers who were under investigation for corruption-related offences improperly accessing confidential information from the QPS computer systems. This case again indicates the vulnerability of the QPS computer systems and further supports the view of the CJC that the QPS needs to take firm action in response.

THE MARKETABILITY AND VALUE OF CONFIDENTIAL INFORMATION

As observed during this and previous investigations, the information that is improperly accessed and/or released is generally confidential information. In Project Piper, the information generally sought related to personal details and/or crime-report information, both of which are classified (using the QPS policies on classification) as in-confidence. This information, which is stored within the QPS and Queensland Transport databases, is not accessible to members of the general public.

In its submission, the QPS suggested that the seriousness of the misconduct revealed during this investigation is lessened because some of the information released by members of the QPS is publicly available and therefore could be otherwise obtained. In closing the public hearing, Mr A J H Morris QC, who represented the Service, stated:

In most instances [meaning those revealed during investigative hearings] we are not talking about people revealing confidential information in the strict term of that sense, that is to say, information which isn't otherwise available, information which is purely held by the Queensland Police Service that you can't get lawfully from anywhere else. Mostly we are talking about people taking lazy shortcuts; people who could go to the Department of Transport and pay a fee and get the name of the registered owner [of] the motor vehicle or go to the electoral rolls and look up the address of a person, go to some other public source and get information publicly available, and just been lazy about it, have looked at the police database because the computer is there on the desk top and it's a quicker and easier and perhaps less expensive way to do it.

Really, what we are talking about in those instances is nothing more than people short changing the Police Service, people obtaining something for free that they should pay for elsewhere. Now, we accept that an entirely different category is where truly confidential

information, information not lawfully available somewhere else, has been misused, but when one looks at the gravity of the situation, how serious it really is, we are simply talking about people not paying full price for the information they got. So whilst the Police Service doesn't in any way resilie from its acceptance that privacy and the protection of information is a matter of great concern, the evidence here doesn't highlight, in the Police Service's submission, any serious or ongoing instances of matters that warrant a reallocation of budget resources away from the Police Service's key areas of concern. (CJC unpub., p. 906)

However, as the QPS has subsequently acknowledged, the policies of the Department of Transport do not allow the release of the name and address of registered vehicle-owners to the general public without qualification (e.g. for insurance purposes).

The QPS submission argued that other databases that are publicly available (e.g. the electoral roll) also contain the addresses of individuals, and therefore the subject officers of this Inquiry were only providing information that could be lawfully accessed elsewhere. However, the CJC makes the following three points regarding that submission:

- Firstly, regardless of what information is available on any other public database, the information held on the QPS mainframe/corporate computer systems is not publicly available and the offence of improperly accessing and releasing information from the QPS mainframe/corporate computer systems is applicable whether the information is an address or a criminal-charge record.
- Secondly, many of these other databases require the individual whose particulars are recorded to volunteer the information; the electoral roll is accurate only when members of the community choose to notify the Government each time they move residence. Failure to do so cannot be easily detected. In other words, the accuracy of publicly available databases is often reliant on citizens volunteering the information.

On the other hand, QPS and Queensland Transport information is often collected rather than volunteered. For example, a person in a motor-vehicle accident must provide certain information, such as name and address, to the attending police officer. The home-owner reporting a break and enter must provide their home address so that police can attend. To obtain a registration sticker for a motor

vehicle, a person must provide an address. In all of these instances the information is obtained involuntarily.

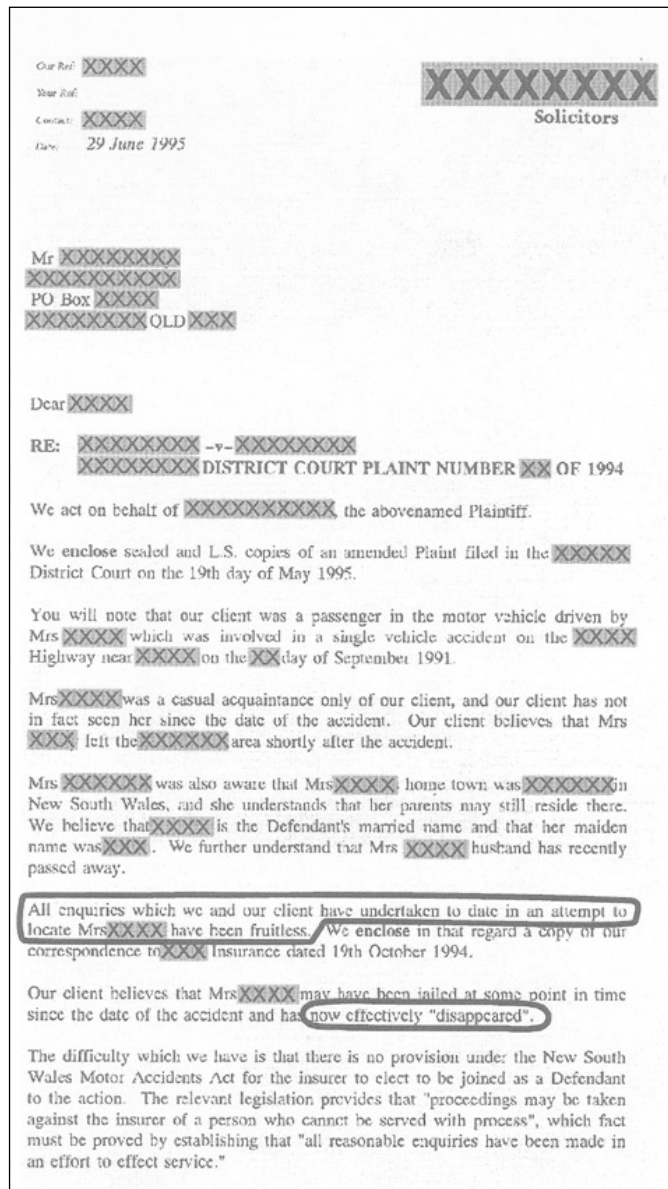
- Thirdly, it is impossible to know which people in the community, or how many people, have chosen not to have their personal details available on publicly accessible databases. It is important to acknowledge the individual's right to control the information recorded on those databases. As emphasised above, this is not so with QPS databases and other restricted government databases, which is one of the reasons that the information available from restricted government databases is sought after.

As discussed in chapter 7, end-users (i.e. the individuals and firms who originally requested the information) were often attempting to locate individuals in order to serve them with court

documents, commence legal proceedings or collect outstanding monies. The difficulty is that these individuals are evading the end-user and often cannot be located by legal means; they are careful not to record personal details on public databases. By way of example, the evidence in figure 4.1, which was seized during Project Piper, indicates the irritation felt by those whose efforts to locate someone are frustrated, and demonstrates why this particular business resorted to employing a private investigator (N2). A finance company that wanted to locate a person urgently stated in its correspondence to a private investigator that it needed to 'make decisions in relation to service of documents and need to know where this man is hiding'.

It is apparent that in many situations the information being sought, such as a current address, is accurately recorded only on restricted

Figure 4.1 — Seized letter stating difficulties in locating an evasive individual



databases such as those held by Queensland Transport and the QPS. This was conceded by the Senior Sergeant at the Inala Police Station, who used the QPS computer systems in the performance of his duties in his second job as commercial sub-agent:

Counsel Assisting: But of course you'd agree with me that the examples that we've seen here [of InI accessing QPS computer systems for secondary employment] are the hard ones, where you've resorted to the police computer to see if you can get any more information [other than through publicly available databases] in order to locate them?

In1: That's correct. (CJC unpub., p. 516)

The President of the Institute of Mercantile Agents (IMA) also explained why the Motor Vehicle Registration Database is more useful for finding evasive people than publicly available databases:

President (IMA): Generally, when doing an inquiry on CITEC, you'll find the registered owner and address. Now frequently the address will be an old address; they'll have left. We know, because our commercial agents have been trying to serve a summons or repossess a car. But, as we all know, when the registration comes up, you've got to pay it and a sticker has to be sent to a new address.

Chairperson: Yes.

President (IMA): And people frequently advise Queensland Transport just before the registration is due to expire ... the person's advertised the new address for the sticker — for the registration sticker to be forwarded to. (CJC unpub., pp. 797–98)

As discussed above, it is often mandatory for members of the public to provide information to the QPS and Queensland Transport. Evidence was heard during this Inquiry of a woman who was hiding from her husband and who was eventually found because she had given her current address to a police officer. The woman detailed her efforts to hide from her husband, who had been violent towards her.

Counsel Assisting: Now, in the years that followed your separation did you take steps to avoid your former husband?

Witness: I did, yes ...

Counsel Assisting: And what sort of steps did you take to avoid him?

Witness: In the beginning I just — first of all I went to a [organisation name] hostel in the

beginning, and it had bars on the windows so that even if I was found he couldn't get in, and after a period of six months, I think it was, they moved us to a normal house and I could only stay there three months, and then we shifted again and we went to — I realised I couldn't stay in normal facilities because he kept finding me so I asked my parents to help me buy a caravan so [I] could move the caravan if I was found. (CJC unpub., pp. 587–88)

The woman then went on to describe how she ensured that her address did not appear on restricted government databases.

Counsel Assisting: And during that period, however, did you maintain a driver's licence?

Witness: Yes, I did.

Counsel Assisting: Did you maintain a motor vehicle?

Witness: Yes, I did.

Counsel Assisting: The driver's licence, did you keep it up to date?

Witness: No.

Counsel Assisting: Why not?

Witness: Because I was scared he could find me.

Counsel Assisting: The motor vehicle, did you keep it licensed in your own name?

Witness: No.

Counsel Assisting: Registered, I mean?

Witness: [Another person] registered it in theirs. (CJC unpub., p. 588)

After several years of successfully 'hiding', the woman was charged with speeding. She was asked to give her current address to the police officers, and the address was entered into the QPS computer system.

Some months later, on 15 November 1995, the private investigator (N2) was instructed by a client who represented the man she was hiding from to locate her. On 16 November, QPS audit trails show a police officer accessing the confidential records of the woman and, in particular, the screen that documented her most recent address. On 17 November, N2 wrote back to his client, giving the woman's address. Within days, the woman became aware that her husband had found her again.

The Inquiry also heard evidence of instances where criminal-charge information, traffic-history information and/or crime-report information,

which is clearly not available to the general public, was provided to the cleaner (N1) at the Nerang Police Station:

Counsel Assisting: In terms of requests for criminal histories for persons did you supply those [to N1]?

N5: Most of the time. (CJC unpub., p. 55) ...

Counsel Assisting: Just getting back to your discomfort in June–July of '98 — was part of that due to the fact that you were, in fact, being asked to provide details of criminal charges or criminal histories?

N4: Yes, generally everything, the whole — the whole — even the addresses was just uncomfortable, the whole thing. (p. 133) ...

Counsel Assisting: So you accept what I'm saying that your — and I think you acknowledge in your evidence today — that your inquiries that you were asked to do by [N1] were rather more wide ranging than simply finding somebody for service of a document?

N6: Yes. At the time that I made the inquiries it was on the basis of locating a person and he has obviously used further information. (p. 152) ...

Counsel Assisting: But, of course, then on occasions you went on to provide him with information about a criminal charge history or a criminal history. That's so, isn't it, on occasions?

N9: On occasions. Yes. (p. 202)

Other officers claimed to have only provided addresses to the cleaner (N1), although the evidence shows that other information, available only on QPS computer systems, was reported back to the end-user. These officers claimed that N1 must have observed the other information on the computer screen as they interrogated the various databases to locate an up-to-date address:

Counsel Assisting: So that really this last search demonstrates [looking at a crime report] that whether you knew it or not at the time [N1] was certainly fishing for more than just an up to date address; would you accept that?

N8: I would accept that. (CJC unpub., p. 91) ...

Counsel Assisting: Well, what's of interest is if you are just on your way through [the computer databases], [N1] seems to have paused for long enough to pick up that she's [name of individual on whom information is being sought] a [name of business] employee and has made four previous complaints. That's a lot of detail beyond trying to find her isn't it? Do you agree?

N7: Yes, but I mean it's not hard to look at and observe, either. (p. 103)

N7 later admits the searches were broader than just addresses:

Counsel Assisting: But in order to go into criminal offences field, not a criminal convictions field, I'll repeat that, but in order to go into criminal offences field, it seems you're going beyond the process of just locating someone for service?

N7: Yes. (CJC unpub., p. 108)

Similarly, in the Fortitude Valley matter, a police officer gave a woman's silent phone number to an acquaintance who worked in a coffee shop he frequented. Again, this was not publicly available information.

For the above reasons, this type of information has a dollar value in some markets (further discussed in chapter 7) and therefore there may be a financial gain or other benefit for individuals who are prepared to improperly access and/or release confidential information.

As noted in chapter 3 ('The Investigation'), the cleaner (N1), then an employee of the QPS at the Nerang Police Station, acknowledged receiving money for information that was provided to him from the QPS computer systems:

Counsel Assisting: Was there a certain amount of money that you would receive for certain types of information?

N1: To the best of my recollection anything between 10 or \$15 for a licence or registration check and anything from 30 up to 40 or \$50 for more detailed or traffic or charge information. (CJC unpub., p. 224)

In other evidence, N1 confirmed that the information he obtained and passed on to the private investigator (N2) came from members of the QPS, and he acknowledged that he did receive both financial and non-financial benefits:

Chairman: You weren't actually serving documents; you were just ... obtaining the information from the police station and passing it on?

N1: Yes ... sometimes there weren't any payments either ... I'd be able to get some information from him [N2] and so it would be a trade-off. (CJC unpub., p. 243)

The Senior Sergeant/Officer-in-Charge (In1) at Inala Station also received money for work he

performed as a commercial sub-agent. His sub-agent work was assisted by the searches he conducted on the QPS computer system during working hours:

Counsel Assisting: Senior Sergeant, you can't be in any doubt that you have used the police computer on more than one occasion to further a commercial venture. You cannot be in any doubt that that's what you have done?

In1: That's correct. (CJC unpub., p. 515)

And then later,

Counsel Assisting: Well, it was simply use of the QPS system for a commercial pursuit? You've agreed with that?

In1: Yes, that's correct. (CJC unpub., p. 521)

Both of these matters are examples of QPS employees receiving material gain as a result of the misuse of the QPS computer systems. They demonstrate the potential value of the information stored in those systems.

Similarly, confidential police information has value to criminals and the potential to compromise an investigation. On one view of the facts, that potential existed in respect of the alleged release of confidential information about the theft of the motorcycle (described in detail on pages 23–25). During evidence, the officer (A) who investigated the matter, an officer with 20 years' experience, agreed that knowledge of some of the details in the relevant CRISP report would have been of benefit to the suspected offenders had they known them. For example, the relevant CRISP report stated that several of the suspects had not been identified. The following exchange occurred in evidence:

Counsel Assisting: You considered that it may be of benefit for a suspect to know whether he [the investigating police officer] knew the suspects had been identified? Was that your view?

A: Yes.

Counsel Assisting: And I think I suggested to you that it may allow a suspect to consider what course of action he or she takes in knowing, may I suggest to some extent, what the state police knowledge is of the offence?

A: That is so. There's a number of quarters I could take with that knowledge.

Counsel Assisting: They may, for example, decide they should work up an alibi?

A: An alibi or perhaps decline to be interviewed at all.

Counsel Assisting: Yes.

A: Knowing that they haven't been identified at all.

Counsel Assisting: Well, they might get together and say, 'We haven't been identified. If we stick together we'll be right'?

A: There's a number of ...

Counsel Assisting: There's a number of possibilities, isn't there?

A: Numerous. (CJC unpub., p. 340)

The above exchange shows the potential for more-serious misuse of information. Some of the CJC operations described earlier document cases where corrupt members have been proven to have accessed and/or released confidential information from the QPS computer systems with criminal intent and, in doing so, to have compromised CJC investigations.

STAKEHOLDER CONCERN FOR THE PROTECTION OF INFORMATION

It is critical that the general community have confidence in the QPS. The initiatives of the Service over the last ten years have most certainly increased public confidence:

- There have been substantial changes to the gender, education and age profiles of recruit intakes to reduce the insularity observed by Fitzgerald (1989) and to create greater diversity within the Police Service, characterised by more mature and responsible individuals. (Police Education Advisory Council 1998)
- An integrated approach has been adopted to achieve ethical decision-making through training and education programs and other initiatives, such as the development of the SELF test. (Appendix I)
- In 1997 the ESC (Ethical Standards Command) was created, a dedicated unit concerned with the continual improvement of Police Service integrity and ethics.
- Proactive management strategies are constantly being developed to deal with complaints and issues of discipline. (CJC 1997b)
- Training in both ethics and management has been developed for personnel in middle management. (CJC 1997b)

Similarly, the ethics surveys conducted by the CJC (1999b) have shown a change in the way junior police officers view several types of misconduct, with most regarding them as more serious and more likely to be detected. These surveys also show an increased willingness to report misconduct when they observe it.

The CJC also conducts surveys on public attitudes towards the QPS. The most recent of these found:

Around 90 per cent of respondents agreed with the proposition that police 'generally' or 'mostly' behave well and most thought that the QPS had 'changed for the better' or 'stayed about the same' over the last few years. There was no increase between 1995 and 1999 in the proportion of respondents reporting dissatisfaction with police behaviour. In both years, very few respondents claimed to be aware of serious misconduct by police. (CJC 2000, p. 1)

The CJC is of the view that the Queensland community should continue to have confidence in the QPS. However, the evidence given at the Inquiry regarding the nature of the confidential information that was improperly accessed and/or released — the personal details of individuals (e.g. addresses, contact details, physical description) and the details of involvement of individuals in the criminal justice system (e.g. criminal-charge records, complaint matters, traffic history) — would most certainly be of concern to the community.

During this Inquiry, two groups with a particular interest in the privacy issue as it relates to the general community — the Queensland Council for Civil Liberties and the Australian Privacy Charter Council — expressed their concern over the issues that had been identified through the hearing process. In respect of the current QPS systems for control and accountability, the President of the Council for Civil Liberties said this:

[The QPS database] is essentially accessible by most if not all serving police officers and by the sounds of it is accessible by other people or has been in practical terms who are not necessarily serving police officers that makes it extremely vulnerable to misuse ... From my reading of the Queensland Police Service evidence they say that they gather huge amounts of data for an audit trail in the order of some terabytes but they don't do anything with it. At page 660 of the transcript from Monday, you as the Chair asked how long it was since the last random spot auditing of information used had taken place and [the QPS representative] said 1997. I mean, that,

quite frankly, is a disgrace ... Again, as I read the Queensland Police Service submission, they say that this has been done on the basis of risk assessment process. And essentially on the basis of that they don't think there's much risk. That's the reality of it however it's dressed up. With respect, we disagree. (CJC unpub., pp. 818–19)

Similarly, the Australian Privacy Charter Council, in their written submission, called upon the QPS to take urgent action:

The gravity of the breaches of trust displayed in Queensland is even greater given that the problem had been identified and well publicised years earlier. There can be no excuse for Queensland Police not being aware of the risk and putting in place better preventative measures and sanctions ... The Police Service needs to urgently address both its monitoring of access to computer systems and, in particular, the disciplinary action it takes against officers and employees who are found to breach the trust placed in them. (2000, p. 1)

Further to the final comment of the Australian Privacy Charter Council, it is important to stress that the QPS has already taken disciplinary action against the majority of subject officers who appeared before the Public Inquiry. Most have been demoted, with several receiving quite significant demotions equalling a number of years career progression.

The QPS also submitted that there was no evidence to suggest that it had in any way compromised its relationship with other organisations. Such a statement is accurate in that no evidence on this point was led. However, there is clearly a risk that other organisations may question the capacity of the QPS to protect confidential information when there is clear evidence that its information systems are open to abuse.

To maintain the confidence of the general public and the organisations that share information with the QPS, the QPS must take action in response to the issues regarding the protection of confidential information available to members of the QPS.

QPS SUBMISSION ON FUNDING

The QPS advised the CJC that the cost of upgrading or maintaining its information systems must be balanced against other community needs and operational priorities, particularly the infrastructure and training requirements that have resulted from the high priority given by successive governments to increasing police numbers. In the QPS written submission it is stated:

The Service will need to consider any recommendations from the Inquiry against current and future State Government and Service priorities. Recommendations with resource implications will need to be considered against other budget priorities ... the practicality of any recommendations will need to be assessed, particularly in light of their potential cost-effectiveness. (QPS submission 2000, p. 26)

In concluding on behalf of the QPS, Mr Morris QC submitted:

Research and feedback obtained by the Queensland Police Service has indicated time and again that people — people, I mean the taxpayers, the voters, the ordinary citizens of this state — want their Police Service to be concentrating, firstly primarily, on police and crime, on getting crime off the streets, in ensuring that people can sleep safe at night in their beds, on making the state a safer and better place to live ...

On one estimate, and I emphasise this isn't the final estimate, the sort of technological response which has been mentioned in evidence in these proceedings could cost anything up to five million dollars. Now, the Police Service doesn't have five million dollars lying around with nothing to do and if it did have five million dollars lying around with nothing to do it would prefer to spend that money by putting fifty more men and women in uniform or having five more police stations rather than spending five million dollars improving security of its database systems. So we — as I say, we make no apology for putting budgetary considerations at the forefront of our response. (CJC unpub., pp. 899–900)

Later, on behalf of the Queensland Police Service, Mr Morris submitted:

So whilst the Police Service doesn't in any way resilie from its acceptance of privacy and the protection of information is a matter of great concern, the evidence here doesn't highlight, in the Police Service's submission, any serious or ongoing instances of matters that warrant a reallocation of budget resources away from the Police Service's key areas of concern. (CJC unpub., p. 906)

While crime reduction is a priority for the community, the community also has an interest in ensuring an honest Police Service that does not violate the very laws it seeks to uphold. The information improperly released often contained the personal details of unknowing members of the

community. The QPS computer systems allow access to all types of personal information, collected for different reasons, about most community members, who should rightly expect that their confidential information will only ever be accessed and/or released for official police reasons and that the privacy of their information is protected to the greatest possible extent.

At the end of the day, this is what the CJC's investigation was all about — police officers acting unlawfully and, in doing so, betraying the trust that the community has placed in them. As Mr Morris submitted:

It is fundamental to our democratic society that people enjoy and are able to enjoy total confidence in those who have the responsibility for administering and enforcing the law of the land. (CJC unpub., pp. 895–96)

The CJC is of the view that the issue of information security falls within the QPS objectives to reduce crime and increase community safety. With regard to estimated costs, this Inquiry heard from industry experts on leading technologies dealing with computer security (e.g. biometrics such as fingerprint-scanning to obtain access to a computer terminal). These are of course quite expensive technologies, and the CJC has been mindful of recommending the most economical strategies to meet the challenge of preventing this type of misconduct.

In its closing submission, the QPS stated that the decision-making process for budget allocation is based on 'how problematic this type of misconduct is'. However, on the opening day of public submissions the CJC also heard that the QPS embraces risk assessment and risk management as fundamental tools in setting priorities for the preventative actions it should take. This being the case, the CJC is of the opinion that the Service should use this approach, in combination with the evidence, submissions and opinions heard before this Inquiry, to determine the priority, and consequently the funding, that it should give to information security, particularly as it relates to the computer systems.

According to the Australian and New Zealand Guidelines on Risk Management (SAA/NZS HB143:1999), risk arises out of uncertainty:

It is the exposure to the possibility of such things as economic or financial loss or gain, physical damage, injury or delay, as a consequence of pursuing or not pursuing a particular course of action.

The concept of risk has two elements:

- The likelihood of something happening; and
- The consequences if it happens. (p. 4)

Risk management can be defined as the culture, processes and structures established to deal with system vulnerabilities that constitute opportunities for misuse or produce adverse effects.

As explained earlier, the prevalence of information-security breaches is very difficult to estimate. However, there is certainly ample opportunity for such misconduct to occur, as the majority of QPS members are given access to the confidential information held on the computer systems. Although users' transactions are logged to an audit trail, none of the users are formally required to record the reasons for the transactions performed. It is therefore difficult and resource-intensive to enforce accountability, a critical feature of good risk management. As this investigation has shown, this allows members of the QPS to use the 'can't recall' explanation when asked to account for their transactions. The use of this explanation by members facing investigation into serious matters is not new; the **Police and Drugs Report** (CJC 1997a) and the **Police and Drugs Follow-up Report** (CJC 1999a) both document how investigations were frustrated by the fact that members were not required to account for their computer use.

Clearly the consequences of improper access and release of information range in their degree of seriousness (see p. 10). One consequence is loss of public confidence, which, although not life-threatening, should not be dismissed as insignificant. A more serious possible consequence would be the death or injury of a person. In such a case, there would not only be loss of public confidence in the QPS, but there may also be significant financial costs to the Service. The potential is there. In two cases heard before this Inquiry, the witnesses gave evidence that they were deliberately hiding from a person they feared; on both occasions officers gave out information about the witnesses' location without turning their minds to the risk involved.

All of the critical issues to be considered in a risk-assessment and risk-management framework are present — opportunity, vulnerability and the possibility of dire consequences for the QPS. Assuming that risk management is the basis on which the QPS makes its budgetary decisions, the CJC is satisfied that there is sufficient risk to justify additional funding for information security.

The CJC appreciates the position of the QPS and the difficulties it faces in managing a limited

budget when there are competing priorities. For this reason the CJC has attempted to make recommendations that do not make unreasonable administrative and financial demands.

In the CJC's view, recommendations of the kind made in this report are inevitable when new information technology and management systems are introduced. The introduction of new technology also brings new risks, and the QPS must continue to give priority to managing information security when planning its acquisition and deployment of assets and information systems. Some comfort can be drawn from the fact that these new systems have themselves resulted in savings in terms of the efficiency with which the QPS's core business is conducted.

CONCLUSION

The CJC has been investigating allegations of improper access to and/or release of information since its inception. From these investigations it has become evident that some subject officers have engaged in this form of misconduct with seriously corrupt intentions, while others have done so for improper, if not actually corrupt, reasons. Regardless of the reasons given for improperly accessing and/or releasing information, what is demonstrated by the CJC experience is that it is fundamentally an invasion of privacy and a breach of law and the trust of these individuals whose personal details have been improperly accessed and/or released. The ease with which an individual member can misuse the QPS computer systems without fear of detection is also disturbing. Without a policy such as a 'reason for transaction' requirement, it is very difficult to enforce accountability.

It is clear that complaints statistics should not be relied upon as an accurate measure of prevalence, nor should the complaints mechanism be considered a comprehensive system of monitoring the improper access to and/or release of confidential information. The CJC is of the view that factors other than prevalence — such as the potential for abuse and the seriousness of potential harm — should be used to determine the response to this type of misconduct. The following points are also important when considering the type of response that is required to deal with the problematic issues raised during this and previous investigations:

- Information accessible on the QPS corporate/mainframe systems is restricted and not generally available to the general public.
- Restricted government information has a

market value because it is particularly useful for locating evasive individuals and includes information (e.g. criminal-charge history) that is not included on publicly accessible databases.

- Given that much of the information available on QPS computer systems relates to individuals in the community, it is important to show the community that they can continue to have confidence in the QPS.
- If the QPS takes no action to solve these problems, when there is clear evidence that its information systems are open to abuse, there is a risk that organisations with which the QPS shares information may question its capacity to protect confidential information.

The QPS submitted that, when developing the recommendations within this report, the CJC should give consideration to the fact that the QPS budget is limited. The CJC has attempted to ensure that the recommendations are financially realistic and appropriate for the QPS. However, it was not possible to make recommendations that are cost-neutral. Just as it is important for the QPS to allocate resources according to its priorities, it is also necessary for the Government to consider its own priorities and, consequently, the policy directions it gives to departments and agencies in relation to information security.

INFORMATION SECURITY IN THE QPS

The information in this chapter was either provided by the QPS in its written submission to the Public Inquiry during the consultation phase that occurred while the report was being drafted, or taken from the QPS Bulletin Board. The Bulletin Board, which is not accessible by members of the public, has electronic versions of the various QPS manuals, as well as general information about the organisation. It was cited numerous times between June and November 2000.

Information is a valuable asset within the QPS and needs appropriate protection. As observed during this Inquiry, the information available on the QPS computer system is a commodity valued by external individuals and organisations. Because of commercial demand, information held by government departments and agencies will always be at risk. The initiatives discussed in chapter 7 ('The Market for Information') are designed to reduce the market for illicit information, but there will always be an element of the community who will inappropriately seek information from those who have access to it. As security and protection become an increasingly high priority for the custodians of information, and as the strategies to protect information become more complex, the illicit trade in information may well become more ingenious.

In chapter 2 ('The Central Issues') the importance of information security was discussed; in particular, the growing importance of protecting information, as reflected in State and Federal Government initiatives, the development of industry standards, the IPPs and the move toward establishing privacy legislation. This chapter is concerned with the progress of information-security initiatives within the QPS. Each of the following areas of information security is discussed in turn:

- information security and the responsible organisational units
- the organisational response to information security

- release of information and accessing the QPS computer system
- conflict of interest: outside employment and associations with private investigators and commercial agents
- disposal of information printed from computer systems
- technology for information security
- use of audit-trail information
- training and education in computer use and information security
- information-security awareness and individual accountability.

INFORMATION SECURITY AND THE RESPONSIBLE ORGANISATIONAL UNITS

The purpose of information security is to provide for the protection of, and ensure the confidentiality, integrity, privacy and availability of, Queensland Police Service information assets, systems and services. (QPS Information Security Policy Development Framework, p. 1, QPS Bulletin Board, 8 June 2000)

In 1993 the QPS established an Information Security Project to develop the Information Security Policy Development Framework. The framework has been reviewed by the QPS and the CJC and was implemented in September 1998. The framework, which is divided into 20 'areas' (shown in table 5.1 on page 42), was based on the guidelines produced by the OECD. It is also consistent with the Australian and New Zealand Information Security Management Standard (AS/NZS 4444.1:1999).

Table 5.1 — The categories and objectives of the QPS Information Policy Development Framework

AREA	OBJECTIVE
1. Security Organisation	To manage information security within the QPS.
2. Information Ownership and Custodianship	To ensure that QPS information and information systems are managed in an effective and systematic manner.
3. Asset Control	To maintain appropriate protection of QPS assets.
4. Information Security Classification	To ensure that all QPS information receives the appropriate level of protection.
5. Personal Security	To reduce the risks of human error, theft, fraud or misuse of QPS information and information systems.
6. Security Incidents	To minimise the damage from security incidents and malfunctions and to monitor and learn from such incidents.
7. Physical Security	To prevent unauthorised access, damage, loss or interference to QPS information systems, services or equipment.
8. Computer Management	To ensure the correct and secure operation of QPS computer and network facilities and to minimise the risk of system failures.
9. Database Security	To control and co-ordinate the use of QPS local and corporate database systems and related data.
10. Network and Communications Management	To ensure the correct and secure operation of QPS network and supporting infrastructure.
11. Security and Computerised Communication Systems	To prevent the loss, modification or misuse of QPS data stored or transmitted on computerised communication systems.
12. Electronic Transfer or Electronic Exchange of Information	To minimise the risks associated with third party access to QPS information and information systems. Agreements must be developed when a significant business need exists.
13. System Access Control	The prevention of unauthorised computer access including user-ID and password management and monitoring system access and use.
14. System Development and Maintenance	To ensure that security is built into QPS information systems
15. Encryption	To prevent loss, modification or misuse of data.
16. Personal Computer Security	To provide security for QPS personal computers.
17. Virus Control	To safeguard the integrity of QPS software and data from the threat of computer virus infection.
18. Business Continuity Planning	To have plans available to counteract interruptions to QPS information systems and business activities from the effects of major failures or disasters.
19. Compliance	To avoid breaches of statutory or contractual security requirements.
20. Security reviews of Information Systems	To ensure compliance with QPS security policies and standards.

Source: QPS Bulletin Board, June 2000

The QPS has two organisational units with responsibility for information security: the ISS (Information Security Section) and the ESC (Ethical Standards Command).

The ISS¹⁴ is located within the Information Management Division (IMD),¹⁵ which is overseen by the Deputy Chief Executive, Resource Management. The ISS has four areas: Information Security Policy and Awareness Training, Investigation and User Access, Information Systems Security Audit and E-mail Systems Administration.

The ISS has both a proactive and a reactive role in preserving information security within the QPS. In discharging its proactive responsibilities, the ISS:

- develops policies and procedures relating to information security to ensure that users are aware of security requirements
- provides awareness training, advice and guidance on issues related to information
- administers the internal and external email systems of all email accounts
- reviews and evaluates information-security requirements for the development or purchase of computer systems and software packages
- reviews and evaluates existing computer systems to ensure that they meet current security requirements
- exercises access control by issuing user-IDs and passwords to authorised users of the QPS Mainframe Systems such as POLARIS and granting users permission to access QPS computer work stations.

The ISS discharges its reactive responsibilities by:

- undertaking, and/or assisting with, investigations of breaches of information security in QPS computer systems, including external computer systems
- assisting officers in their investigations by the provision or verification of computer evidence
- performing security audits of the information system to ensure that the technical aspects of the systems are working as intended.

The ESC was established in 1997 to promote ethical behaviour, discipline and professional practice in the QPS through deterrence, education and systems improvement. The structure of the ESC (shown in appendix L) has four branches: Inspectorate and Evaluation

Branch, Internal Investigations Branch, Ethical Practice Branch and Internal Audit. The role of the ESC includes:

- reviewing, determining compliance with, and reporting on such issues as:
 - the systems established to ensure compliance with QPS policies, plans, procedures, laws, regulations and delegations of authority where they have a significant impact on operations and reports
 - the means of safeguarding assets from loss, theft and/or fraud and, where necessary, the existence of QPS assets
 - the economy and efficiency with which resources are managed and used
 - operations and programs to ascertain whether results are consistent with established objectives and goals
- investigating allegations of misconduct and breaches of discipline, including suspected unethical conduct
- developing educational strategies to promote, reinforce and engender in all employees a full understanding of the expected standards of ethical behaviour
- enhancing ethical standards for employees of the QPS by developing corporate policies, practices and strategies that prevent or discourage unethical conduct
- actively overseeing and investigating complaints against members and other police-related incidents
- administering the disciplinary system of the QPS.

Investigations by the ESC or the CJC of alleged improper access and/or release of information from the computer systems are supported by the ISS through the provision of relevant audit trails.

THE ORGANISATIONAL RESPONSE TO INFORMATION SECURITY

The QPS has two high-level committees that can attend to information-security issues: the Information Steering Committee (ISC) and the Risk Management Committee. The QPS also has a centralised information service through the Police Information Centre (PIC).

The ISC — This committee was established in response to the Queensland Government Information Standard 16 (Department of Communication and Information, Local Government and Planning 1999), which requires

the establishment and maintenance of the committee. The Government recognised that information management is not an IT problem but a business matter requiring a strategic whole-of-organisation approach. The Standard requires the committee to be chaired by the Chief Executive Officer or Deputy and clearly states that:

The agency Information Steering Committee (ISC) has responsibility and accountability for ensuring:

- that the use and application of the agency's information resource is consistent with the corporate directions and business functions of both the government as a whole and the agency as a single entity;
- that the agency's deployment of information technology is directed at the effective and efficient management of the agency's information resource;
- that appropriate security measures are developed, endorsed, instituted and monitored. (1999, p. 2)

The QPS ISC meets every three months on matters relating to information management, system performance and project status. The ISC is chaired by the Commissioner of Police and comprises the following members:

- Deputy Chief Executive, Operations
- Deputy Chief Executive, Resource Management
- Assistant Commissioner, Operations Support Command
- Assistant Commissioner, Southern Metropolitan Region
- Director, Finance Division
- Director, IMD
- Assistant Commissioner, Director Operations, CJC
- Director, Administration Division
- Manager, Information Planning Branch, IMD

The Risk Management Committee — This committee has been established to perform the tasks that the Government requires departments and agencies to undertake (as specified in the Financial Management Standard 1997). The committee is chaired by an Executive Officer nominated by the Commissioner and consists of members selected from the following areas:

- Deputy Chief Executive, Operations
- Deputy Chief Executive, Resource Management
- an Assistant Commissioner nominated by the Commissioner
- Director, Office of the Commissioner
- Superintendent, Inspectorate and Ethical Practice Branch, ESC
- Director, Finance Division
- Director, Administration Division

The role of the Risk Management Committee is to:

- oversee and review the development of the risk-management policy to be endorsed by the Commissioner of the Police Service
- provide direction and guidance for the implementation of the risk management policy, as well as for the acceptance of the change that this will involve
- ensure that management accountability for risk management is supported by appropriate systems and control procedures
- ensure that appropriate systems are in place to collect data that will enable the Risk Management Committee to monitor the effectiveness of risk management over a period of time.

Regions, Commands and Directorates may also establish Risk Management Committees to assist in the implementation of risk management at the local level.

The Operational Procedures Manual (OPM) also has a chapter (15) on the Risk Based Assessment System, which provides comprehensive guidance on how the system operates and how to implement it.

The PIC — The PIC is located within the IMD and provides police, members of the public and external agencies with a 'one-stop-shop' for a range of information and services relating to offences, suspects, offenders, wanted persons and persons who are the subject of court orders. The PIC consists of the Information Service Unit, the Warrant Bureau and the Information Support Unit. The PIC also has an overseeing role in relation to the release of crime reports through CITEC CONFIRM.¹⁶

Section 1.10 ('Release of Information') of the OPM provides clear and specific guidelines to members on what can be released and by whom.

The effect of the orders, policies and procedures is that the majority of requests for information are to be made through the PIC. There is little discretionary decision-making for individual members and the majority of requests can and should be referred to the PIC. Members who are unsure can call the appropriate help/assistance line.

RELEASE OF INFORMATION AND ACCESSING THE QPS COMPUTER SYSTEMS¹⁷

The QPS policies and procedures on accessing the QPS computer systems and information disclosure are found in a number of documents. The following sections explain those provisions as they appear in the OPM, the Administration Manual and the Human Resource Management Manual (HRMM). The QPS information-security video and handbook, which provide guidance to members, are also described.

OPM: Section 1.10 ('Release of Information')

The OPM includes orders, policies and procedures, defined in the OPM thus:

Order — an order requires compliance with the course of action specified. Orders are not to be departed from.

Policy — A policy outlines the Service attitude regarding a specific subject and must be complied with under ordinary circumstances. Policy may only be departed from if there are good and sufficient reason(s) for doing so. Members may be required to justify their decision to depart from policy.

Procedure — A procedure outlines generally how an objective is achieved or a task performed, consistent with policies and orders. A procedure may outline actions which are generally undertaken by persons or organisations external to the Service.

The following order is made under section 1.10 of the OPM in respect of release of information:

Members are not to release information other than:

- (i) in accordance with a structured scheme;
- (ii) in accordance with Service policy;
- (iii) with the approval of an Executive Officer;
- (iv) in compliance with ss. 109 or 119R of the Police Powers and Responsibilities Act; or
- (v) in accordance with the legislative requirements of the Freedom of Information Act.

It is also clearly stated that it is an offence under the PSAA to improperly disclose official information. An extensive range of orders, policies and procedures are provided in the OPM, and these clearly state under what circumstances a member can release different types of information (shown in table 5.2 on page 46).

Administration Manual: chapter 4 ('Information Security') and chapter 11.5. ('Documents Available to Members of the Public from the PIC')

Chapter 4 of the manual has 20 sections covering the various areas of information security (as shown in table 5.1, above). The broad organisational policy on information security (section 1 of chapter 4) states that:

The Queensland Police Service must manage information security through the establishment of:

- a management framework to initiate and control the implementation of information security within the Queensland Police Service
- an information security management committee to approve security roles, and to co-ordinate the implementation of security across the Queensland Police Service
- a source of specialist information security advice available within the organisation
- suitable liaison points for dealing with security incidents, and
- multi-disciplined approaches to information security.

It is also through policy (section 13 of chapter 4) that access to computer systems is discussed:

Access privileges are allocated on a 'need to know' basis, i.e. a person has a genuine 'need to know' if, without access to certain information, they would be hindered in the proper and efficient performance of their duties.

Members are not entitled to see or obtain information merely because it would be convenient for them to know or by virtue of their status, rank, office or level of authorised access.

Members must not:

- access any computer system unless as part of their official duties (being those actions which a person is authorised to perform as part of their duties as a member of the Queensland Police Service)

Table 5.2 — Sections of the OPM on release of information

SECTION	ORDERS, POLICIES AND PROCEDURES
I.10.1	Requests by members of the public for their own police certificate, record of charges or criminal-history particulars.
I.10.2	Third-party requests for personal-history information or personal information held on records of charges.
I.10.3	Requests by members of the public and external organisations for information held in crime report records.
I.10.4	Requests for copies of statements.
I.10.5	Requests for information related to traffic incidents.
I.10.6	Requests for Queensland vehicle registration and driver’s licence details.
I.10.7	Requests by members of the public for information concerning vehicle/property suspected stolen.
I.10.8	Requests by victims of crime for information about the investigation.
I.10.9	Requests by persons other than victims of crime for information about the investigation.
I.10.10	Requests for historical information and research assistance.
I.10.11	Information sought by the media for public broadcast.
I.10.12	Information released by police seeking public assistance in the investigation of incidents and crimes.
I.10.13	Requests for statistical information.
I.10.14	Requests for information from other government departments, agencies or instrumentalities.
I.10.15	Requests for information from other law-enforcement agencies.
I.10.16	Documentation required by the courts.
I.10.17	Requests by members for information about themselves.
I.10.18	[Spare]
I.10.19	Requests for interviews with members of the QPS. Requests from insurance companies. Requests from other persons, agencies or organisations.

- use another member’s user-ID and password to access any computer system or
- divulge their password to any other person.

Many sections and areas of this chapter are incomplete or missing. The QPS has indicated that this chapter is still being developed.

HRMM Code of Conduct: section 10.12 (‘Improper Access or Use of QPS Information’)

The Code states that ‘it is the view of the Service that there is no excuse for members to betray the

public trust by making any unauthorised, improper or unlawful access or use of any official or confidential information available to them in the performance of their duties’. Such actions are prohibited under the Code, and ‘where any member breaches this provision they must expect that the Service will institute appropriate disciplinary or criminal proceedings’. The Code states that this type of activity is viewed as misconduct. QPS expectations of its members in relation to public comment and their communication with the community are also outlined.

HRMM Procedural Guidelines for Professional Conduct: section 4.10 ('Improper Access or Use of QPS Information')

These guidelines state that 'the unauthorised and improper access, use or release of investigative information to a suspect or accused person is not permitted' and that 'members are to ensure that all legislative requirements and Service instructions governing the release of information are complied with'.

The Information-Security Awareness Video

The video was produced by the ISS for Information-Security Policy and Awareness Training. The video makes it clear, in simple terms, that the computer system should be used for 'authorised work-related matters only' and that curiosity and favours for friends or families are not appropriate reasons for using it. The video also states that, with one exception, officers should never conduct searches on behalf of anyone else, the exception being radio operators who perform searches on behalf of officers working on the street. The viewer is also instructed to log off all systems, networks and email systems before leaving a terminal. Other issues covered are email use, password protection, Internet use, downloading of software and the use of floppy discs. The video also instructs computer users to apply the SELF test (appendix I) when unsure whether their intended action is appropriate. The video has been distributed state-wide to all training officers.

The Information Security Awareness Handbook

The handbook is produced by the ISS for Information-Security Policy and Awareness Training. It is similar in content to the video and is to be used in conjunction with it.

CONFLICTS OF INTEREST

The issue of conflict of interest and outside employment is discussed in the Code of Conduct and the Procedural Guidelines for Professional Conduct:

HRMM Code of Conduct: section 10.6 ('Conflicts of Interest'), and section 10.9 ('Outside Employment')

The Code requires members 'to perform their duties in such a manner that public confidence and trust in the integrity, objectivity and impartiality of the Queensland Police Service and its members is preserved'. Further, where a conflict of interest does occur, the member is to disclose the details of that conflict to their supervising Executive Officer. Members are not to engage in any employment, while on leave or

otherwise, if this employment:

- (i) interferes with the effectiveness of the performance of their duties;
- (ii) creates or appears to create a conflict of interest; or
- (iii) reflects adversely on the Service.

HRMM Procedural Guidelines for Professional Conduct: section 4.4 ('Conflicts of Interest'), and section 4.5 ('Outside Employment')

These guidelines re-state the comments made in the Code of Conduct and outline the procedures for obtaining authorisation for outside employment. Police officers or recruits are not permitted, without the support of the Executive Director of Operations, to accept employment in a managerial, administrative, consultative or public-relations capacity with a security-services company or act on behalf of, or as an agent of, a security-service company seeking to employ police. The QPS has taken this position because this type of employment has the potential to create a conflict of interest that may reflect adversely on the Service. For other categories of outside employment, members are required to provide written advice to their supervising Assistant Commissioner, Director or Executive Manager. There must be sufficient information to allow the authorising officer to apply the assessment criteria (shown in appendix M) in determining the appropriateness of the outside employment.

Policies and procedures on associations with private investigators and commercial agents

Although there are policies and procedures on conflicts of interest and informant management, there are no specific QPS policies or guidelines on associations with private investigators or commercial agents.

DISPOSAL OF INFORMATION PRINTED FROM COMPUTER SYSTEMS

The QPS has a number of policies and procedures for the disposal of information and records. These are included in the QPS Administration Manual in chapter 13 ('Records Management') and in the QPS Records Retention and Disposal Handbook. These policies and procedures comply with the **Libraries and Archives Act 1988**. Further guidelines on the classification and management of classified information are given in chapter 4 ('Information Security') of the Administration Manual.

Areas of the QPS with high risk have local

procedures for the release, destruction or disposal of information. For example, the Bureau of Criminal Intelligence has standing orders stating that 'no paper with written official material is to be placed in rubbish bins. This material, along with computer print outs, is to be shredded daily.'

The QPS has recently adopted a new security classification system for information. This system divides all information into the categories of 'Highly Protected', 'Protected', 'In-Confidence' and 'Unclassified'. As this Inquiry is concerned with only 'In-Confidence' material, disposal provisions for 'Highly Protected' and 'Protected' information will not be discussed here.

Under the new system, the 'In-Confidence' security classification should be assigned when the unauthorised disclosure, loss, modification or misuse of the information has the foreseeable potential to compromise the privacy of any person or create misinformation. An example of information that should be classified as in-confidence is personal information that should not be released without the knowledge and authority of the person concerned, other than by a process of law (chapter 4, section 4.1(c), Administration Manual, QPS).

Hard-copy in-confidence documents are to be kept in a safe and secure environment (section 4.1(i)i, Administration Manual, QPS) and should be placed in a locked bin to await disposal. In-confidence material is to be shredded under the supervision of the Information Custodian (section 4.1(k), Administration Manual, QPS).

THE TECHNOLOGY OF INFORMATION SECURITY

All corporate/mainframe information systems and specialised information systems implemented at the QPS are subject to access control. Access is provided to individuals on a need-to-know and right-to-know basis. Access to QPS data is controlled by user registration, user-ID, password, transaction and transaction-group management, terminal-ID and the log-in process.

All QPS System and POLARIS users are obliged to change their password every 90 days. Access and privilege are dependent on the role of the user. Currently there are approximately 10,500 users with access rights to POLARIS, and 11,500 with access rights to the QPS System.

It is standard practice for all corporate/mainframe systems to keep a full audit trail of all user activity. The audit trail collects full details of all user queries, modifications, deletions and entries. A subset of the audit trail is written to a command or activity log. When there is a need to examine

audit trails, the command or activity log is interrogated first: if there is a 'hit' or 'match', the full audit trail is extracted.

In the case of POLARIS, the keystrokes of a user can be played back in real time. This capability was used during the hearings on an officer who accessed the personal details of an individual to obtain a silent phone number. The real-time play-back clearly demonstrated a pause at the screen displaying the phone number. When questioned, the officer admitted that the pause was indicative of the time it took for him to write the phone number down.

Audit trails are currently retained for seven years; however, on the basis of an analysis of search requests and use over a two-year period, the ISS has recommended a 10-year retention period. It has also indicated that a hold has been placed on the destruction of audit trails for operational matters where court cases have not yet been finalised (i.e. they are held for over seven years).

The mainframe/corporate systems also have automatic log-out after a set period of non-use. The POLARIS system has a two-stage automatic log-out. After 15 minutes of non-use, users need only re-enter their password to regain access. After 30 minutes of non-use, the system is automatically logged out completely. The QPS System has automatic and complete log-out after 60 minutes of non-use. Users who have been completely logged out need to re-enter user-ID and password to enter the systems again.

USE OF AUDIT-TRAIL INFORMATION

During the public hearing there was discussion on the use of audit-trail information:

QPS representative: Some of the methods we use in our area where we actually check on specific instances where people have accessed information, individuals have accessed information. And an example of that may have been a recent one where there was a media article in relation to a police officer and we conducted a spot audit on whether anyone had checked the personal details of the officer mentioned in the media article ... (CJC unpub., pp. 656-57)

And then later:

Chairperson: You see, we've been told that other police services have ongoing audit processes that systematically audit, you know, the majority of officers for example on a yearly basis, in terms of their use of the computer system, to check whether there's been some

misuse. But the QPS hasn't got an ongoing program like that, although from time to time there has been some random auditing.

QPS representative: That's as I understand it, yes.

Chairperson: Do you know how long it is since the last random spot auditing of information used?

QPS representative: I think the actual date was 1997 and it was related to an incident on the Gold Coast or a media article on the Gold Coast. Yeah, that's probably the most recent one. (CJC unpub., p. 659)

Since the hearing, the QPS has submitted that over the last few years it has performed three types of audits:

- examination of the computer accesses of the accounts of persons appearing in the media
- examination of the computer transactions of a member who has performed excessive transactions
- random examination of a select group of members.

The QPS has also indicated that, since the closure of the public hearings, three audits have been conducted. Each audit involved a selection of officers (e.g. at a particular station) whose computer-transaction records were inspected for 'exceptions' (e.g. excessive transactions). Any officers identified as 'exceptions' were asked to provide the reasons for transactions.

It was also noted that, in 1994, the then Commissioner's Inspectorate conducted random audits on information systems use as part of its inspection program. The audit trail for the two weeks before an inspection would be obtained. At the inspection, members would be required to provide reasons for accessing the computer systems. This practice was discontinued in September 1996.

As part of the risk-management procedures for the Academy, proactive inspections are performed on police recruits and detective training students. The ISS provides, on a monthly basis, extracts of audit trails for the purpose of checking system use. The Manager of the ISS indicated that officers from the section have commenced a program of going out to the Academy, armed with the audit trail of students' computer use from the day before, and showing exactly what information is recorded on an audit trail. Students are then questioned as to their reason for access.

On average, the ISS receives approximately 400 requests for audit trail searches in a twelve-month period. These requests are made for the following purposes:

Technical reasons

Twenty per cent of requests are to obtain assistance with data problems, application problems and system failure.

Operational police investigations

Forty per cent of requests are from operational police officers who need to clarify details about a certain activity (when, for example, the time of an offence is important, or where the time information received and recorded on the computer system may be of assistance) or to identify transactions that were performed some time ago and have now become important (e.g. to check on a person who was the subject of a routine search and who has now become a suspect for an offence).

Investigations into possible misconduct

Forty per cent of requests are from the CJC, the ESC and/or QPS Commissioned Officers for investigation of allegations of system misuse (e.g. unauthorised access and disclosure of information).

TRAINING AND EDUCATION IN COMPUTER USE AND INFORMATION SECURITY

The Police Recruit Operational Vocational Education (PROVE) Program provides comprehensive training to police recruits on information security. Recruits are required to read the Information Security Awareness Handbook and watch the accompanying video. They are also instructed to watch the video on information security produced by the NSW Police Service. All recruits are required to complete an assignment that focuses on the legal and ethical use of the police computer systems. The Police Operational Conversion Course (POCC), which is the training provided to recruits who have prior policing experience, uses the same computer training module as is used in the PROVE program.

The First Year Constable (FYC) Program is compulsory and includes one 'competency' on the police computer system. This competency refers to 'improper disclosure of information' and the students must be able to explain the legal rights of a person providing information and the jurisdictional policy and procedures for ensuring information security.

The Constable Development Program (CDP) is a three-year program that prepares Constables for promotion to the rank of Senior Constable. In

Year 3, students are questioned on a case study that concerns the unlawful disclosure of information.

The Competency Acquisition Program (CAP) provides distance education and computer-based training for all members of the QPS. It includes modules on ethics and the use of notebooks, diaries and registers, but no specific module on information security, privacy and the 'need-to-know' principle. It was indicated during the Inquiry that a current training-and-awareness initiative of the ISS is the development of a CAP module in information security.

The Management Development Program, which qualifies officers for promotion to the ranks of Sergeant, Senior Sergeant and Inspector, also has an emphasis on ethics but no specific component on information management and security.

The Investigations and Intelligence Training Program provides specialist training for the development of plain-clothed officers and ongoing training for detective/specialist areas. It has several specific sessions that relate to information security and lawful access to, and use and disclosure of, information.

Civilian staff of the QPS are required to complete an induction course that includes a 30-minute session on computer security, legislative, policy and ethical aspects of information security and disclosure of information.

INFORMATION-SECURITY AWARENESS AND INDIVIDUAL ACCOUNTABILITY

Civilian staff are required to sign a confidentiality agreement, shown in figure 5.1, when appointed to a position. The agreement clearly outlines the responsibilities of the civilian appointee in the area of information security. In contrast, police officers are not required to sign a confidentiality agreement.

All members who log on to the QPS System or POLARIS are exposed to a warning screen that indicates the conditions of access to and use of the computer system. The warning screen for POLARIS is shown in appendix N and the screen for the QPS System in appendix O. They are similar in content and clearly state: 'You are NOT authorised to access information for personal reasons' and 'The information contained on this computer system is confidential and must not be disclosed to unauthorised persons'. It also indicates that audit trails are recorded and can be retrieved.

CONCLUSION



The QPS has commenced an approach to information management that accords with the Australian and New Zealand Information Security Management Standard (AS/NZS 4444.1:1999) and the guidelines provided by the OECD. It has been only a short time since the Information Security Policy Development Framework was introduced in late 1998. To date the QPS has:

- established two organisational units responsible for information security — the ISS and the ESC (the latter is responsible for integrity and ethics in the Service more generally and conducts investigations into alleged breaches of information security)
- established the ISC and the Risk Management Committee
- developed a central information service, the PIC, for all individuals and organisations that request information
- developed policies on information security and published them in the OPM, the HRMM and the Administration Manual
- implemented a program of collecting full audit trails on the corporate/mainframe computer systems
- adopted the role-and-access model as an information-security control mechanism
- developed a video and handbook for information-security training and education
- incorporated information security into the training programs for junior officers and new staff members.

The QPS is to be commended for its approach to information security to date; however, it must remain vigilant in ensuring that information security is properly protected. This is particularly important given the increased reliance on information systems and the move towards policing strategies such as intelligence-driven and problem-oriented policing, which require speedy access to information.

Information-security policies need to be clear, concise and well defined. They must be supported by appropriate control and compliance systems that are sophisticated enough to ensure that the QPS meets its statutory obligations to protect information and ensure the privacy of individuals. There is still much to be done to ready the QPS for the next decade so that it can prevent information breaches of the type revealed by this and previous investigations. The measures that will be needed to do this are discussed in the following chapter.

Figure 5.1 — Confidentiality agreement signed by QPS civilian employees

	QUEENSLAND POLICE SERVICE Information Security Section, Information Management Division 100 Roma Street, Brisbane, QLD, 4000 G.P.O. Box 1440, Brisbane, QLD, 4001 TELEPHONE (07) 3364 6670 FACSIMILE (07) 3221 4060	 QP 408 07/00
---	--	--

**CONFIDENTIALITY AGREEMENT
FOR QUEENSLAND POLICE SERVICE EMPLOYEES**

I, _____

being attached to _____,

hereby acknowledge that I have been given access to certain areas of the Queensland Police Service computer system(s).

I will ensure that my computer password(s) are confidential, known only to myself.

I will not leave my terminal unattended when logged into the computer system(s) with my user-id and password.

I agree to perform only such transactions on the computer system(s) as may be authorised in the course of my duty and to treat all information which I obtain from that computer system as confidential.

I will not perform any unauthorised transactions on the computer system(s), nor will I release or otherwise deal with any information from that computer system in any manner which has not been approved by my superiors.

I am aware that all transactions that I perform on the computer system(s) are recorded and such recordings can be retrieved if the need arises.

I acknowledge that if I breach this agreement I may be liable to have action taken against me under The Police Service Administration Act 1990, Section 18 of The Human Resource Management Manual, Section 85 (Disclosure of Official Secrets) or Section 408D (Computer Hacking or Misuse) of the Criminal Code Act 1899.

I have read and agree to abide by the agreement as set out on this form.

Dated at _____ this _____

day of _____ Year _____

Signature _____

Witness to Signature _____

Q U E E N S L A N D P O L I C E S E R V I C E

IMPROVING INFORMATION SECURITY IN THE QPS

The QPS is to be commended on the measures it has taken to strengthen information security. However, as was demonstrated by this Inquiry, the issue of information security needs constant review. With each advance in technology comes an equal responsibility to develop strategies and systems that will combat the new security threats it brings with it. Not surprisingly, one of the greatest threats presented by integrated information systems comes from those individuals who have access to the information.

The revolution in information technology has brought rapid improvements in business processes, efficiency and productivity, but many organisations, particularly in the public sector, have been slow to deal with the associated risks. This problem has been exacerbated by software designers who have focused on the functionality of the programs they design: a lower priority has been given to the development of effective security features to protect the information that is entered into the various programs and databases. Often it is not until a computer information system is in use that the risks to information security are fully exposed.

The response to identified security risks should be multi-pronged:

'I want to make a brief point about technological versus organisational measures. Technological measures alone are not going to solve problems of confidentiality. Organisational measures are necessary to complement them to ensure that they are effective. The same goes the other way around. Organisational measures are insufficient. Technology must be used to complement organisational measures. A data security strategy has got to address both of these ...'
(Mr Roger Clarke[18] speaking at the Just Trade Seminar held by the ICAC, 1992b, p. 66)

The QPS similarly emphasised the importance of a strategic approach to the issues of concern in its written submission (2000, p. 5):

The Service is acutely aware of the need to implement policies and practices designed to

maintain the security of its information. The issue is where to strike the balance between establishing practices that may unduly impede the work of operational police while ensuring that systems are in place to protect information against unauthorised access. This problem is not unique to the Queensland Police Service; public and private organisations at the local, state, national and international levels face similar issues. Over the past decade the Service developed security practices and policies as its technological capabilities increased. In many areas, the Service operates at levels not exceeded elsewhere in Australia. It is unlikely that in the current decade technology may develop as rapidly as it did in the 1990s. Organisations will be required to invest significantly. Security issues will not be solved by a single program or policy and an adaptable and multi-pronged approach will be called for.

The CJC's Inquiry identified a number of areas for improvement or change to enhance the information security of the QPS computer systems. The recommendations in this report are made in consideration of the observations of this and other inquiries and investigations, having regard to the fact that information systems will become increasingly important to the operational performance of the QPS. While the Service reaps the benefits of these advances, it will also need to ensure that organisational and technical responses are continually developed to protect computer information systems from being used improperly.

This chapter commences by describing the methodology that has been employed to assess QPS information-security management as it relates to confidential information accessible through the computer systems. The remainder of the chapter concerns areas where improvement or change can enhance QPS computer information security, protect against the type of misconduct uncovered during this Inquiry and deal with future security threats. The issues are discussed under the following headings:

- An organisational response to information security
- The location of the Information Security Section
- Corporate/mainframe computer access for authorised users
- Corporate/mainframe computer access using another person's user-ID
- Conflicts of interest: outside employment and associations with private investigators and commercial agents
- Disposal of information printed from corporate/mainframe computer systems
- The technology of information security
- Systematic internal audit
- 'Reason for transaction' requirement
- Information-security awareness and individual accountability
- Training and education in information security.

METHOD OF ANALYSIS

In conducting this review, consideration was given to the current QPS orders, policies, procedures and guidelines, particularly in terms of their effectiveness in preventing the misconduct that was revealed. Other material that was considered when developing the recommendations included:

- relevant legislation
- best practice in information security as specified through the standards and practices of other jurisdictions and industries
- the written and oral submissions received from interested stakeholders.

The CJC also drew upon its previous experience in investigating this type of misconduct to identify the problems and issues that consistently emerged.

Recommendations have also been made in view of the evidence given on several issues of concern to the CJC:

- A number of officers denied the allegations when initially interviewed by investigators.
- A significant number of officers did not make full disclosures until forced to do so under oath at a public hearing.
- At the Nerang station it appeared that providing information to the cleaner, N1, was an accepted practice.

- None of the subject officers at the Nerang station refused to give information to N1. Some of the reasons given were that:
 - it appeared to be an accepted practice
 - they felt obliged to because of their junior status
 - they formed the opinion that N1 was of good character and felt a kinship because he is an ex-police officer.
- In all the years that N1, at the Nerang station, was obtaining confidential information from police, no complaints were ever received despite the fact that there was continuous movement of staff in and out of the Nerang station.
- Evidence was given that there was discussion between some subject officers about resolving to just 'tough out' the CJC investigation.
- One officer felt justified in conducting improper searches to check the probity of an acquaintance or just out of curiosity about people he once associated with.

Given the above issues, it is clear that organisational controls and policies alone will not prevent misconduct of this kind and will not be sufficient to detect it. To act on the above findings and to ensure compliance with QPS policies and procedures, effective monitoring and detection systems are also required. Strategies for promoting positive cultural change should also be incorporated.

Recommendations have been developed to meet the future needs of the QPS for security of its computer information and to position it as a 'lead' organisation in security of computer information in the area of policing. In making the recommendations, the CJC has been mindful of costs, but not at the expense of the information-security objectives of the QPS. It is essential for the QPS to ensure that, over the next few years, information security continues to be a high priority in strategic planning, budget and resource allocation to give effect to its own security objectives and to the recommendations in this report.

AN ORGANISATIONAL RESPONSE TO INFORMATION SECURITY

As discussed in chapter 2 ('The Central Issues'), the responsibility for promoting information security and establishing it as a high priority must be taken at a corporate level. The Australian and New Zealand Standard on Information Security Management (AS/NZS 4444.1:1999) states that

information security is a business responsibility that should be shared by all members of management. The standard suggests that organisations establish a management forum to discuss information security and to 'ensure there is clear direction and visible management support for security initiatives ... That forum should promote security within the organization through appropriate commitment and adequate resourcing' (p. 5).

Decisions relating to information security must be made at the highest level within the QPS because of their cost implications and their importance to the efficiency and integrity of the QPS information systems. With the constant changes and improvements to the computer information systems, it is necessary to constantly review information security within the QPS.

The 'forum' would be a management committee concerned with information-security matters that extend beyond the issues identified during this Inquiry. It would be concerned with the security and protection of all information, not just that which is stored on QPS computer systems. The information-security areas that require attention are:

- security policy
- information-security infrastructure
- information-security risk analysis and management
- asset classification and control
- personnel security
- physical and environmental security
- communications and operations management
- access control
- systems development and maintenance
- budget and funding
- business continuity management
- compliance.

The committee should be charged with the broad responsibilities for:

- a) reviewing and approving information security policy and overall responsibilities;
- b) monitoring significant changes in the exposure of information assets to major threats;
- c) reviewing and monitoring security incidents;
- d) approving major initiatives to enhance information security. (AS/NZS 4444.1:1999, p. 5)

The QPS has recognised the need to have a management committee with responsibility for improving information security, as shown by the information-security organisation policy, outlined in chapter 4 (section 1) of the Administration Manual:

That the Queensland Police Service must manage information security through the establishment of ...

- an information security management committee to approve security roles, and to co-ordinate the implementation of security across the Queensland Police Service

It is a good time for the QPS to implement the policy stated in chapter 4 (section 1) of the Administration Manual and establish a management committee to oversee information security. However, since the first draft of this report, QPS representatives have indicated that management has decided that such a step is not necessary. The QPS is of the view that the current corporate governance structure, which includes the ISC and the Risk Management Committee (discussed on pages 43–44), subsumes all the responsibilities that would normally fall to an information-security management committee. The priority, in the view of the CJC, is for these responsibilities to be adequately discharged on an ongoing basis. While the CJC prefers the concept of an information-security management committee, particularly for an organisation as large as the QPS and one that relies heavily on information systems in its day-to-day operations, it is a matter for the QPS to determine what type of structures and systems it institutes to achieve this goal.

An important initial step in the organisational approach to information security is the development of a comprehensive set of orders, policies and procedures on all aspects of information security. It was observed that many sections from chapter 4 ('Information Security') of the Administration Manual are incomplete. This is an important set of policies that instruct and guide members of the QPS to ensure that they act appropriately and legally. The QPS should, as a priority, ensure that the orders, policies and procedures for information security are finalised and the completed manual released to its members.

RECOMMENDATION 6.1 — ENHANCING THE CORPORATE RESPONSE TO INFORMATION SECURITY

6.1.1 That the Queensland Police Service, through the establishment of an information-security committee, or through current

committee structures, ensure that the following duties are discharged on an ongoing basis:

- review and approve information-security policy and overall responsibilities
- monitor significant changes in the exposure of information assets to major risks
- review and monitor incidents affecting information security
- recommend to the Commissioner of Police major initiatives to enhance information security.

6.1.2 That, as a matter of priority, orders, policies and procedures for information security be finalised and released to members of the Queensland Police Service.

THE LOCATION OF THE INFORMATION SECURITY SECTION

The ISS (Information Security Section) is currently located within the IMD (Information Management Division). The IMD is responsible for both information management and information security.

The ESC (Ethical Standards Command), which was established in 1997, is responsible for maintaining ethical behaviour, discipline and professional practice in the QPS through deterrence, education and systems improvements. Similarly, the ISS is concerned with deterrence, education and systems improvements as they relate to information security. Given the overlap in the roles and responsibilities of the two areas, it is logical to place the ISS within the ESC. Such a move would send a strong organisational message concerning the importance of information security from the perspective of ethical conduct, integrity and professionalism. It would also serve to ensure that the information-security imperative is not lost in the race to install new computer systems.

There are also sound operational reasons for transferring the ISS to the ESC. The ISS presently provides significant operational support to the ESC in respect of its investigations into allegations of computer misuse and the unlawful dissemination of information. In addition, the ISS will be required to assist with any future internal audit program that is likely to be conducted by the ESC.

There should also be some consideration given to the grouping of functions that are located under the ISS. It may well be the case that, if the ISS were to move to the ESC, one or two functions may be more appropriately left within the IMD,

for example administration of email systems.

Such a proposal will require careful consideration. On the basis of what is known, however, the CJC believes information security in the QPS will be improved by incorporating the ISS into the ESC.

RECOMMENDATION 6.2 — REVIEW LOCATION OF THE INFORMATION SECURITY SECTION

That the Queensland Police Service review the organisational structure as it relates to information security, giving particular consideration to the placement of the Information Security Section within the Ethical Standards Command so that the information-security goals and objectives of the Queensland Police Service can be more readily achieved.

CORPORATE/MAINFRAME COMPUTER ACCESS FOR AUTHORISED USERS

The Administration Manual provides that access privileges are allocated on a 'need to know' basis and that members must not access any computer system unless it is for the purpose of their official duties (see p. 45). Despite this, some officers admitted to accessing information on the QPS computer systems out of curiosity. While this is certainly less serious than unlawfully accessing and then releasing information, it remains unlawful.

In another departure from policy, several officers were of the belief that they could pass on confidential information to another person if they believed the recipient to be 'of good character'. The OPM does concede that policy may be departed from where there are good and sufficient reasons; however, the belief that the recipient is of good character is not a 'good and sufficient reason'.

In one example, the subject officer, Senior Constable FV1, stated that he was asked by an acquaintance, FV3, to confirm whether or not a woman (FV2), whose welfare he was concerned about, had taken out a DVO. Senior Constable FV1 agreed to do so. During questioning, the Commission asked Senior Constable FV1 what authority he had relied upon to make the search and pass on the information:

Counsel Assisting: He's concerned for her welfare. Well, is that a sufficient basis to allow you to confirm the existence of an order that somebody professed to have concern for her welfare?

FV1: In this incident, yes. (CJC unpub., p. 183)

Senior Constable FV1 also provided an unlisted phone number to FV3:

Counsel Assisting: And you believed that in this instance you supplied the unlisted telephone number in good faith?

FV1: On the basis of the information that was provided to me by FV3. (p. 184)

This officer failed to understand not only that he was not authorised to access the police records, but that disclosure of a silent number is clearly improper in such circumstances.

The majority of subject officers brought before the Inquiry from the Nerang station made similar errors of judgment. These officers routinely provided information from the QPS computer systems to the station cleaner (N1), who worked as a process-server and for a private investigator (N2). All of the subject officers believed N1 to be of good character, and unquestioningly accepted his reasons for wanting to procure information. Again, while many of these officers recognised that it was wrong to provide the information, they clearly did not understand that they themselves, in most cases, were not permitted to access those records on the computer systems. Although authorised users, they did not have a genuine operational reason to be exercising their access rights.

As was explained in the report of the National Police Research Unit (NPRU),¹⁹ **A Standard Law Enforcement Information Security System: Guidelines for Law Enforcement Agencies** (1995), the clearance to view material up to a certain classification does not justify a person's viewing any material about which they do not have a genuine and authorised 'need to know'. It is particularly important that members of the QPS understand the 'need to know' principle, given the considerable information to which they have access. It is therefore recommended that an order (as defined in the OPM) be promulgated, directing that a user may access the computer systems only for reasons of official police business. Clear explanations of what constitutes appropriate access, with examples, should be provided as guidance to members.

During the Inquiry it became clear that there are differences of opinion as to just what is an appropriate reason to access the computer systems. The QPS should make a public statement on whether it is appropriate for a member to look up records:

- of a person with whom they are wishing to

associate or are considering a relationship

- of a friend or relative where involvement with the police is suspected
- of an individual who has been mentioned to them and about whom they are curious
- of an individual who is about to be employed by a friend or relative
- to check vehicle-registration particulars before buying a vehicle to determine if it has been in an accident
- of prospective neighbours to see if they are part of the 'criminal element'
- as a part of a 'self-training' exercise.

The decision as to whether these are acceptable reasons should be formally communicated to all members of the QPS.

The QPS must also state its position on whether it is acceptable for members to look up their own records. The policy and procedure set down in section 1.18.17 ('Requests by Members for Information about Themselves') of the OPM states that information in documents such as personnel files should be provided to members only in very limited cases. This section states that members should access their personnel information through the procedures stated in section 25.3.3 ('Access to Personnel or Human Resource Information') of the HRMM. Members are instructed to direct their inquiries initially to the appropriate personnel officer. There is an absence of other guiding policy or procedure if members wish to look up those records of their own that are not part of their personnel record (e.g. charge record, traffic history, outstanding warrants).

In developing clear and specific guidelines, the QPS should consider the rights accorded to members of the public for accessing information on the QPS computer systems. The QPS has extensive policies and procedures on dealing with requests from the public for information, and on the charges that will be incurred for searches. In answering the question of whether a member of the QPS should be permitted access to any records, even his/her own, there must be some consideration given to the access rights accorded the general public. Why should a member be able to access his/her own record by virtue of his/her position, when the average citizen cannot? As noted in one report of the Office of the NSW Ombudsman:

The Senior Constable is mistaken in his belief that he can access his own details at will. Authority to access any specific information rests with the Police Service, not with the

person whose details are stored therein. An officer has no more right to check information contained within the system concerning himself than any member of the public has to look up his own criminal history or any criminal has to check what information is stored in the Police Service intelligence database concerning his illegal activities. (1995, p. 9)

Any decision by the QPS on what type of access is acceptable must be clearly communicated to members. It needs to be firmly conveyed to members that access to the QPS computer systems as an 'authorised' user does not entitle searches to be conducted for non-police work, even if they are only conducted out of curiosity, or for personal reasons. It is important that members understand that this type of conduct is unacceptable regardless of whether the accessed information is improperly passed on to an unauthorised person or not.

RECOMMENDATION 6.3 — PREVENTING INAPPROPRIATE ACCESS TO QPS COMPUTER SYSTEMS

6.3.1 That the Queensland Police Service communicate through an Order that:

- authorised users are not permitted to access any computer system unless they do so as part of their official duties (such duties being those actions that a person is authorised to perform as a member of the Queensland Police Service)
- members are not entitled to access any computer system merely by virtue of their status, rank, office or level of authorised access.

6.3.2 That the Queensland Police Service formally provide members with specific examples of appropriate and inappropriate reasons for access. The examples should include the inappropriate reasons proffered by members who have come under investigation for accessing police computer systems.

CORPORATE/MAINFRAME COMPUTER ACCESS USING ANOTHER PERSON'S USER-ID

Another security problem observed during the Inquiry was that of officers leaving open terminals unattended, thereby providing the opportunity for another member to conduct a search under their user-ID. In one bracket of evidence, that relating to Senior Sergeant In1 at Inala Police Station (see pp. 20–21), it was clear that inappropriate searches were conducted by the Senior Sergeant under the user-ID of several other officers. This

situation arose because it is common practice to leave a terminal unattended while it is still logged on to the QPS corporate/mainframe systems. The following exchange occurred during evidence:

Counsel Assisting: Have you encountered the situation where you've sat down in front of a live computer obviously because someone else had been using it before you?

N4: Yes.

Counsel Assisting: Is that common?

N4: Not unusual. (CJC unpub., p. 480)

Several other officers also gave evidence to this effect. This practice is clearly a case of very poor information security, particularly given that a quick and simple keystroke will log the user out of the corporate/mainframe systems.

The same problems have been encountered in other jurisdictions. A representative of the South Australian Police (SAPOL) told the CJC of an investigation into an officer who was alleged to have supplied criminal records to a private investigation agency. In that case the officer used as his defence the fact that leaving computer systems open is accepted practice. He claimed that this practice must have resulted in others using his user-ID to access the records in question. Fortunately, other evidence was able to incriminate this officer. He was convicted and later imprisoned. This is another example of the problems that arise when officers are not compelled to take individual responsibility for information security.

The QPS computer systems do have automatic log-out times. However, they are quite generous and range from 15 to 60 minutes. There are no effective sanctions against members who leave their terminals open and unattended. Although the QPS Information Security Video advises users not to leave their terminal unattended while logged into the QPS computer systems, there are no supporting orders or policies to reinforce this advice.

In marked contrast to the situation that applies to police, civilians are required to sign a confidentiality agreement upon commencement of their employment with the QPS (see p. 51). By signing the agreement, they agree not to leave their terminal unattended when logged into the computer system(s) with their user-ID and password. The agreement raises awareness and reminds users of their responsibility. It also provides a basis on which disciplinary action can be taken. The use of contracts to raise user awareness of individual accountability is discussed later in this chapter (pp. 73–75) so will

Figure 6.1 — Example of a room in a suburban police station



not be further commented on here.

The CJC considered but rejected a proposal to reduce the automatic log-out time because of the inconvenience to those officers who work within the corporate/mainframe systems for extended periods but may have a period of non-use while reading a document or working in another system. Furthermore, it was considered undesirable to abrogate the individual member's responsibility for maintaining security. It is possible that reduction of automatic log-out times may also result in members taking less responsibility for logging out.

For two reasons, the computers that are currently used by the QPS cannot be 'locked' using a 'password protect' screen:

- In many areas of the QPS (such as 24-hour police stations), computers are a shared resource located in a common area. This is depicted in figure 6.1, which shows an example of a common working area for operational police in a suburban police station. The two computers at the rear of the room (circled in the picture) are shared by all officers working in the common area.

In this case it would not be appropriate for members to lock terminals using a 'password protect' screen, as it denies access to other employees. In very busy stations where computer resources are lacking, it would be inappropriate for any member to lock a terminal. Under these circumstances, where resources are scarce, computers should be completely logged out and left ready for the next user.

- The Apple Macintosh computers currently in use by the QPS do not have a 'password protect' screen feature to allow the individual terminal to be locked while the user is still logged in. Further, as mentioned above, even if this function did exist, only members who have their own computer could use it.

When, in the future, the QPS changes its standard desktop operating environment, it will be an opportunity to ensure that the lock-screen function is available and used by members where appropriate (e.g. by members who have their own computer).

The only way to deal with this problem now is to place responsibility on the individual users and require them to ensure that they always log out of the computer system if they have to leave the terminal unattended, and to prohibit access to computer systems using another person's user-ID.

RECOMMENDATION 6.4 — PREVENTING USE OF ANOTHER USER-ID

6.4.1 That the Queensland Police Service develop and implement an order that requires users to always log out of the computer system if they have to leave their computer terminal unattended.

6.4.2 That the Queensland Police Service develop and implement an order prohibiting access to computer systems by means of another person's user-ID.

6.4.3 That, in developing any future standard desktop-operating environment, the Queensland Police Service give careful

consideration to mandatory use, where appropriate, of a 'lock screen' or equivalent facility at the desktop level (e.g. for those members who are allocated their own personal computer).

The effective implementation of the above recommendations also requires commitment at the station and district levels. The risk-management system adopted by the Service requires that officers-in-charge and supervisors adopt a proactive approach to enforcing the requirement to log out of computer systems when leaving terminals unattended.

RECOMMENDATION 6.5 — RISK MANAGEMENT TO ENSURE THAT MEMBERS LOG OUT

That, as part of risk management at the district and local levels, officers-in-charge and supervisors ensure compliance with the requirement to log out of computer systems before leaving a terminal unattended.

CONFLICTS OF INTEREST

During the course of its investigations, the CJC established that 11 serving police officers of the QPS held a private investigator's licence. None claimed to be using the licence for secondary employment.

One of those who held a private investigator's licence was Senior Sergeant In1. He admitted to using the QPS computer to assist him in locating debtors on behalf of a debt-recovery agency.

Private investigators rely heavily on receiving and exchanging information. Therefore it is hardly surprising that Senior Sergeant In1 succumbed to the temptation to avail himself of the information on the QPS computer systems when trying to locate debtors. Clearly his duty to maintain confidentiality in respect of information on the QPS databases was in conflict with his duty to make every effort to locate debtors on behalf of his secondary employer.

Such conflicts may arise in other ways. For this reason, the QPS has established a procedure whereby members can apply for outside employment and has established policies that help both members and their supervisors to decide whether or not the proposed outside employment is appropriate. However, such guidance is unnecessary here, as there can be no doubt that secondary employment that involves locating people or providing services to organisations and individuals who wish to locate people is a conflict of interest for any member of the QPS, or indeed for any government

department or agency where employees have access to confidential and personal information.

Certain types and classes of secondary employment should simply be prohibited by the QPS. It is the considered view of the CJC that members of the QPS should not be permitted to hold a licence as either a commercial agent or sub-agent, private investigator or employee of an organisation performing this type of work.

RECOMMENDATION 6.6 — PREVENTING CONFLICTS OF INTEREST THROUGH OUTSIDE EMPLOYMENT

That the Queensland Police Service promulgate an order:

- prohibiting members from being registered and/or licensed as a private investigator, commercial agent or sub-agent and/or process-server
- prohibiting members from undertaking employment with any private-investigation, process-serving or other agency/organisation that is concerned with locating people or obtaining personal and/or confidential information.

The only exception to the above order should be for those members who obtain the formal authorisation of the Deputy Commissioner of Police to engage in this type of secondary employment after applying to establish that theirs is a special case.

During the ICAC Inquiry (1992a) it was noted that many private investigators were ex-police officers. Similarly, the cleaner at Nerang (N1) and the private investigator (N2) were both ex-police officers. In giving evidence, some of the subject officers suggested that the fact that N1 was an ex-police officer was a factor in their decision to release information to him:

Counsel Assisting: On what basis did you perform those checks for the station cleaner?

N7: Initially when I was at Nerang he approached me for information as to vehicles or persons he had seen around the neighbourhood. And I was — also known to me that he was an ex South Australian police officer who had an interest in his neighbourhood and what was going on at work. (CJC unpub., p. 97)

Evidence was also heard that N1 was closer to station members because he was an ex-police officer:

Counsel for the witness: And how was he [N1] regarded by your fellow officers?

N7: He was well liked and he was considered trustworthy and reliable. It was known he was

an ex police officer and he appeared to have a good rapport with the senior sergeant at the time.

Counsel for the witness: Did he in all of those circumstances then seem closer to the police than a cleaner would ordinarily be?

N7: Definitely. I think he could be trusted a lot more than other people who weren't police that worked at the station. (CJC unpub., p. 109)

It is disturbing that such blind trust could be placed with someone simply by virtue of their previous occupation.

In its written submission, the QPS stated that it would be a mistake to assume that any contact between officers and people in vocations such as private investigation and process-serving is always sinister and undesirable. It quite fairly points out that the receipt of information from security firms and private investigators can be extremely beneficial to criminal investigations. It was also pointed out that some people in these vocations have 'high moral fibre' because they are ex-police officers. The CJC certainly does not disagree with any of these points. What does concern the CJC is the undue influence that an ex-police officer can have, as was seen in the case of N1. The QPS acknowledged this and proposed an approach to the problem:

At the same time, it has to be recognised that a close working relationship between serving officers and people who pursue such vocations has the potential to place officers in a situation of temptation. The Service proposes that this whole issue be considered by the Ethical Standards Command, in consultation with the Criminal Justice Commission. (QPS Submission 2000, p. 24)

The CJC is very supportive of this approach.

RECOMMENDATION 6.7— ADDRESSING THE ISSUE OF ASSOCIATIONS BETWEEN POLICE OFFICERS AND PRIVATE INVESTIGATORS OR PEOPLE IN SIMILAR OCCUPATIONS

That the Ethical Standards Command of the Queensland Police Service, in consultation with the Criminal Justice Commission, review the issue of associations between police officers and private investigators or individuals in similar occupations, to develop policies and strategies to deal with the issue effectively and provide guidelines for police officers on what kind of association is appropriate.

DISPOSAL OF INFORMATION PRINTED FROM CORPORATE/MAINFRAME COMPUTER SYSTEMS

The appropriate method for disposing of information printed from computer systems depends, in part, on the classification of that material. Under the QPS classification policy (Administration Manual, chapter 4, section 4.1(c)), the information on the computer system, such as personal information, criminal-charge history and traffic, should be classified as in-confidence. It follows that, in accordance with QPS policies, hard-copy documents containing such information should not be put in waste-paper bins but stored in locked containers until their disposal. Disposal is to be under the supervision of an authorised member.

A disturbing observation made during the Inquiry was the practice of the cleaner at Nerang station, N1, of taking paper copies of in-confidence documents from waste-paper bins. In his role as the cleaner, N1 was required to remove rubbish from the waste-paper bins and destroy it in an incinerator at the back of the station. N1 was clearly not supervised in this practice and admitted to removing paper copies of in-confidence material from waste-paper bins:

Counsel Assisting: . . . it's been suggested by some witnesses that you may have adopted this practice: requested a police officer for information, observed a print-out being created of the information requested and biding your time to a period later in the day and on your rounds of cleaning up the office fishing out the police print-out keeping it and destroying all other surplus material according to your task as a cleaner; what do you say to that suggestion as a possibility for your behaviour?

N1: It's a possibility, yes.

Counsel Assisting: . . . do you agree that without the knowledge of the some officers you removed police print-outs? [Witness claims privilege but is directed to answer the question.]

N1: Yes. (CJC unpub., p. 236)

Police computer print-outs were found in the documents seized from N1.

Members must clearly understand that information on the corporate/mainframe systems is classified as, at a minimum, in-confidence. This is particularly important because officers access and print information from the computer systems on a daily basis. The requirement to manage that information according to its classification needs

to be understood by all members of the QPS. In-confidence material to be destroyed is to be shredded under the supervision of the Information Custodian (section 4.1(k), Administration Manual, QPS).

To address this issue, the QPS should:

- draw up guidelines, incorporating examples, on how information from the computer systems should be classified and consequently handled
- place an additional condition on the computer warning screens for access to the corporate/mainframe computer systems stating that all users are required to treat information within the computer systems as having a classification of at least in-confidence unless otherwise specified
- insert an in-confidence notice on each computer screen/record within the corporate/mainframe computer systems that contain such information, and on all paper-copy print-outs from the corporate/mainframe computer systems.

RECOMMENDATION 6.8 — ENSURING THE APPROPRIATE DISPOSAL OF PAPER COPIES OF IN-CONFIDENCE INFORMATION

6.8.1 That the Queensland Police Service formally provide guidelines, with examples, on how information from the computer systems should be classified to ensure that members understand which disposal methods are suitable for paper copies containing this type of information.

6.8.2 That the warning screens for access to Queensland Police Service corporate/mainframe computer systems include a condition that all information in these computer systems has a minimum classification of in-confidence unless otherwise specified, and that hard-copy print-outs should be disposed of in accordance with current QPS policies.

6.8.3 That an in-confidence notice be inserted on each computer screen that may contain in-confidence information within the Queensland Police Service corporate/mainframe systems to ensure that the in-confidence classification is included on all printed hard copies.

THE TECHNOLOGY OF INFORMATION SECURITY

There is a range of technological innovations that can be implemented to protect information systems and detect misuse. These are shown in table 6.1.

One of the obvious and powerful information-technology features to enhance information security is that of role determining access — in other words, a person's role determines the level of access they are granted. The role and access management approach used by the QPS entitles most police to have access to the corporate/mainframe computer systems. The QPS argues that any further restriction on access will compromise operational policing. In particular, unrestricted access promotes and encourages intelligence-driven and problem-oriented policing.

While the CJC is always supportive of proactive policing initiatives, it must be recognised that in the present case unrestricted access leads to greater security risks from internal threats. To maintain this level of access there is a need for additional measures to ensure the security of the information held on the QPS computer systems. Policies and procedures represent only one aspect of information security and need to be complemented by appropriate technological controls. Technological controls enforce information security in a way that cannot be achieved by policy and procedures alone.

Consideration was given to technological control systems such as the use of biometric information for access and the adoption of smart cards. While these technologies are gradually being incorporated in the private sector, it would create a significant financial burden for the QPS if the CJC were to recommend their introduction at this time. The CJC has chosen to limit its recommendations to those measures that can be implemented with the current computer systems. Furthermore, the problem of greatest concern to the CJC is improper access to and release of information by authorised users. Technologies such as smart cards do not solve this type of problem; they are more effective in preventing the use of computer systems by unauthorised individuals. Other IT initiatives such as alert monitoring will be much more effective in dealing with the issues raised by this Inquiry.

The CJC identified three IT measures that can be adopted by the QPS within the current system and will significantly improve the monitoring and detection of improper computer access. It is recommended that these capabilities be introduced within the next three years. Given that

Table 6.1 — Examples of technological initiatives to improve information security

ACCESS RESTRICTIONS	DETECTION AND MONITORING
Role determines access	'Alert' monitoring for selected records or transactions
Workstations not useable without certain information, e.g. biometric information (such as fingerprints) and password	Audit software that detects changes in user patterns
Print-outs provided only to nominated printers and/or addresses	Ceilings on the number of transactions to detect excessive use
Bars placed on selected records (e.g. those relating to sexual assault)	'Alert' warning on transactions that the system can do but are not approved for the particular user
AUDIT-TRAIL ACCESSES	INCREASING WARNINGS
Purpose of access	Warning after every request is made and before data are displayed
Nature of data accessed	Warning displayed and printed with all information
Whether a print-out was requested	Electronic acknowledgment of information-security issues for sensitive databases before access
Whether a copy-and-paste was undertaken	Electronic acknowledgment of information-security issues for sensitive databases before access
Number of failed log-ins	Electronic copies and their print-outs have security classification clearly stated
Unauthorised attempts to access particular databases	

all government departments and agencies are required, under the Financial Management Standard 1997, to undertake strategic information-systems and assets planning, the CJC is of the view that three years is a suitable period in which to plan and implement these measures.

1. 'Alert' monitoring for selected records and transactions — 'Alert' monitoring is a system feature that advises the designated supervising authority when particular information is accessed or when certain transactions are performed (e.g. a member accesses the record of a media figure who has been in trouble with the police). It is a highly effective mechanism for detecting improper access and would be a comprehensive strategy to meet the QPS's obligation to protect information. It would also greatly assist the ESC and the ISS in discharging their duties. Victoria Police (VICPOL) have an 'alert' monitoring function built into their computer programs and have reported that it is a very useful tool. It removes the need to constantly check records that have been identified as particularly at

risk and is an integral feature of audit programs targeting records of well-known individuals whose personal details may be accessed out of curiosity.

2. Barring access to selected records — On occasions, the sensitivity of information will demand that routine access be barred. Examples are the records of a high-profile individual who is the subject of a sensitive criminal investigation, victims of certain crimes (such as rape), and the records of individuals who have reported death threats against them. In these cases, barring access to records may be necessary to protect information. Where information or records are barred, a procedure will need to be established that allows members to be provided with that information after they have demonstrated a valid 'need to know'. Exceptions to barring should be for selected individuals who have an ongoing 'need to know' because of operational requirements (e.g. investigators or police prosecutors). Similarly, members found to have attempted access to barred information/records should be asked to give their reasons for

attempting access. This would act as another system for monitoring and detection.

The South Australia Police use bars on records that relate to sensitive murders and rape-victim details. The identity of people who attempt to access barred information is recorded, and they are asked to explain.

3. 'Alert' system for excessive transactions — This is a simple 'alert' system that can be extremely useful in monitoring computer systems for excessive levels of access. Some concern was raised that this type of alert system may result in busy officers being unfairly targeted for audit and investigation. However, the use of benchmarks and the implementation of a properly instituted system of 'alert' monitoring for excessive transactions, together with a clear understanding of the need for accountability, would counteract this tendency.

An effective system would have different thresholds for different classes of employees. For example, traffic officers would have a significantly higher threshold for access to vehicle-registration information than the typical general duties police officer.

In most cases any investigation would begin by approaching the subject officer's supervisor, who may be able to justify the level of computer inquiries, thereby obviating the need for any further investigation.

It is important that the QPS continue to be vigilant in assessing and considering new IT measures to assist in the protection of information and the detection of inappropriate use through the strategic planning process. As IT innovations emerge, there will be a corresponding need for the development of appropriate and effective control mechanisms.

RECOMMENDATION 6.9 — TECHNOLOGY FOR INFORMATION SECURITY

6.9.1 That, as a matter of priority, the Queensland Police Service progressively incorporates information-technology capabilities within the next three years to:

- install an 'alert' monitoring feature for selected records and transactions
- install a 'barring access' function for selected records and information
- develop and implement a system for detecting excessive transactions by authorised users.

6.9.2 That, as part of strategic planning, the Queensland Police Service continues to monitor the development of new IT capabilities that can assist in the protection of information and the detection of inappropriate use.

SYSTEMATIC AND ONGOING INTERNAL AUDIT

It is well documented within corruption-prevention literature that internal audit is an effective deterrent and detection mechanism. Certainly users are more likely to be tempted to misuse the computer system if they believe there is little chance that they will be detected.

The CJC regularly surveys FYCs (First Year Constables) concerning their views on ethical conduct and the disciplinary and complaints process. Respondents are presented with 10 scenarios illustrating various forms of unethical conduct and asked several questions about the scenarios, including 'How would you rate the likelihood of an officer who engaged in such behaviour being caught?'. The scenarios are shown in table 6.2.

Data collected before this Inquiry began demonstrate that junior police officers believe it is unlikely that an officer would be 'caught' for conducting a vehicle-registration check to obtain the address of an attractive women seen driving a car (scenario 7). As shown in figure 6.2, FYCs rate the likelihood of being detected for improper computer access as described in scenario 7 as unlikely.

The views of the FYCs are probably correct, given the evidence gathered during this Inquiry. This perception was confirmed by one subject police officer:

Chairman: So although that screen [referring to computer warning screen] tells you that the checks can be audited, at the time you made these checks you didn't really think that there was much chance of anyone picking it up?

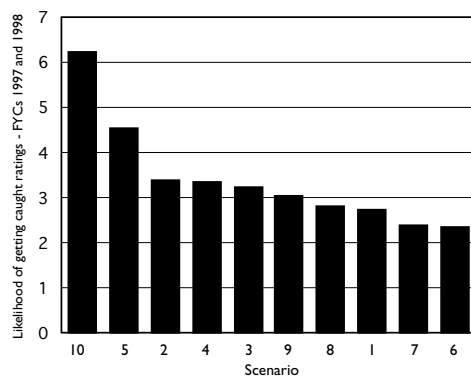
NQ1: It would have been safe to say it, yeah. (CJC unpub., p. 633)

In its submission (pp. 48–49), the QPS stated that auditing is used, but there is no systematic and ongoing program of audit specifically for computer access.

Table 6.2 — Scenarios in the CJC survey on ethical conduct

Scenario 1	Off-duty officer tried to avoid Random Breath Test
Scenario 2	Officer at bottle shop break-in pockets cigarettes
Scenario 3	Officer retaliates against youth who assaulted female officer
Scenario 4	Accident by police misrepresented in report
Scenario 5	Words added to suspected rapist's statement
Scenario 6	Pick-up of personal items outside of patrol area
Scenario 7	Registration check to get details of an attractive woman
Scenario 8	Officers accept cartons of beer for Christmas party
Scenario 9	Officer forcibly moves youth on
Scenario 10	Officer engages in 'skimming' from drug exhibits

Figure 6.2 — Perceived likelihood of being detected for improper and unethical conduct



Source: Research and Prevention Division, CJC

Notes:

1. Rating scale is 1 to 7, with 1 being 'not at all likely' and 7 being 'very likely'.
2. Subjects were First Year Constables surveyed in 1997 and 1998.
3. N size for each scenario ranged from 263 to 268.
4. A brief description of each scenario is given above.

It is well documented that best practice in information security is characterised by follow-through compliance checking, with the policies and procedures in place. As the Office of the NSW Ombudsman commented in their written submission (2000, p. 20):

83. For officers intent on improperly accessing information, the most powerful disincentive is the prospect of being found out. This is only likely to occur if such officers are aware that frequent random audits are occurring.

84. Given the harm that may arise from improper accesses, it is important that audits be conducted frequently to maximise the likelihood that improper accesses are detected early.

As the Inquiry heard, other jurisdictions have commenced systematic internal audit programs for computer use:

- **NSW Police Service** — With the introduction of a new computer system in 1994, the NSW Police Service commenced a systematic random audit program of accesses made to the system. The auditing processes are conducted at two levels: the Audit and Evaluation and Internal Affairs conduct targeted and random audits, whereas Commanders/Managers perform quarterly checks of 25 per cent of personnel and their computer accesses. All staff are audited annually. The NSW Police Service also uses IT initiatives to assist in the audit process. Special audit software continuously monitors the systems to detect any attempts at improper accesses.

The Office of the NSW Ombudsman reported that the commencement of the random audit of computer accesses resulted in an increased number of internal police complaints. This indicates that there are clear benefits in having an internal audit program on computer access. The NSW Police Service reported at the Inquiry that 27 police (serving and former) had been charged either criminally or by summons for a total of 147 offences relating to 'unlawful access to computer'. As a long-term consequence of information-security initiatives, the NSW Police Service reports that the rate of complaints about the provision of unauthorised information and misuse of the computer system is now declining.

- **SAPOL (South Australia Police)** — A member of Information Systems and Technology Service is the designated data-integrity and security-systems officer, who conducts about 200 separate audits per year. These include audits on the accessing of records of high-profile individuals who have appeared in the media. SAPOL is also moving toward giving some audit responsibility to divisional managers.
- **VICPOL (Victoria Police)** — VICPOL conducts both random and targeted auditing of computer access to the Law Enforcement Assistance Program (LEAP), which is conducted by both the LEAP project office and an internal audit team.

The individuals representing each jurisdiction reported positive results from implementing internal-audit processes. Some of the above programs are random, meaning that all members have an equal probability of being selected for an audit. Other programs are targeted, for example the one used by SAPOL, which involves checking accesses to the records of high-profile individuals. Both types of audit, random and internal, are useful for detecting improper access to confidential information held on the computer systems.

Random audits provide a powerful deterrent effect, as has been observed in the literature on the use of random breath-testing. Targeted audits are extremely useful in high-risk areas. The technological functions recommended above will greatly enhance the ability of the QPS to conduct effective targeted audits.

This is an opportune time for the QPS to make a commitment to introduce a program of systematic and ongoing internal audits. The program should have both random and targeted components. The issue of how to design such a program is a matter for the QPS.

To promote greater area/unit responsibility, local areas should incorporate within their risk-management processes a system of local internal audits of access and use of QPS computer corporate/mainframe systems. The provisions for this are set out in chapter 15 ('Risk-Based Assessment System') of the OPM

RECOMMENDATION 6.10 — SYSTEMATIC AND ONGOING INTERNAL AUDIT

6.10.1 That the Queensland Police Service give higher priority to the use of audit strategies to prevent this type of misconduct by developing and implementing a systematic and

ongoing internal audit program, which is both random and targeted, of access to and use of the computer corporate/mainframe systems.

6.10.2 That, as part of the risk-management process, managers and supervisors incorporate a program of local internal audit of access and use of computer corporate/mainframe systems.

'REASON FOR TRANSACTION' REQUIREMENT

During the course of this investigation and similar inquiries elsewhere, many officers claimed to have no recollection of the computer inquiry in question or the reason why it was conducted. In the case of the Nerang Police Station, the CJC was only able to go behind this response because it had conducted an extensive investigation with the benefit of documentation that it obtained by means of a search warrant. This is not always possible.

In the absence of any other means by which to prove or disprove whether access was appropriate, an investigator must accept the 'can't recall' defence. Similarly, audits of computer access can only be conducted effectively if users are required to demonstrate why they accessed the computer systems.

The New South Wales experience on reason for transaction

The NSW Police Service is the only jurisdiction to implement a mandatory recording of reason for transaction Service-wide. There are some parallels between the development of that system and the history of this debate in Queensland.

In 1992, the ICAC released a report on an investigation of improper access and release of confidential government information. The investigation revealed a highly active illicit information trade that involved public servants from various government departments and agencies, including the NSW Police Service. It revealed the inadequacies of information-security management in many departments and agencies.

In May 1993, the NSW Ombudsman released a provisional report on one matter of this nature (Office of the NSW Ombudsman 1994). It was recommended that, to solve these problems, the NSW Police Service insert a 'reason for transaction' field that users would have to complete before they could obtain access to the computer system. The NSW Police Service rejected the recommendation because:

- the insertion of such a field would generate costly overheads

- people would just enter general reasons that would not assist with investigations
- corrupt individuals would not enter their real reasons for logging on.

The NSW Ombudsman considered these arguments and concluded that they did not justify rejection of the recommendation. The NSW Police Service continued to argue that a 'reason for transaction' field within the computer system for every transaction would not be cost-effective as an anti-corruption measure, particularly given that over 12 million accesses are made to the system each year. The NSW Police Service's concern was acknowledged by the Ombudsman's Office and an alternative proposal was recommended, namely that a policy be formally adopted whereby all users of the computer system will be held accountable for accesses that occur under their passwords.

The NSW Police Service responded by issuing a Commissioner's Notice (94/110) requiring all members to keep a written record of the reason for computer inquiries. However, a later Commissioner's Notice (95/8) served to override the mandatory nature of this requirement:

The Service is conscious [of the requirement] to balance the needs of practical policing with the necessity to account for the reasons why inquiries are made. The Service is also aware it is not necessary to record the reason for every inquiry when records show the validity of the access. It is necessary, however, where practicable, for members of the Service, who have cause to access the computer, to record the reason for entry, particularly if they consider the inquiry might be the subject of an audit or is of a contentious nature. (Office of the NSW Ombudsman 1995, p. 4)

The Office of the NSW Ombudsman again stated that the problem regarding improper access and release of information by police officers had not abated:

In subsequent discussions, this Office was assured by police management that complaint figures relating to improper computer accesses would decline as a direct result of this newly-introduced re-education program targeting police culture. This has not, in fact, occurred ... (1995, p. 1)

Of concern to the Ombudsman was the fact that the NSW Police Service had rescinded its initial mandatory requirement to record reason for transaction, therefore leaving it to the subjective judgment of the member concerned as to whether

supporting documentation for a transaction was required. Furthermore, the Commissioner's Notice did not carry the force of a Commissioner's Instruction for the purposes of taking effective disciplinary action against members shown to have improperly accessed computer systems. The 1995 Report of the NSW Ombudsman cited numerous cases where subject officers did not record a reason for transaction and used the 'can't recall' defence despite the Commissioner's Notice.

Since that time, as acknowledged by the NSW Ombudsman, the NSW Police Service has taken effective initiatives for information security. The Service has commenced the move toward mandatory recording of reason for access. On 29 July 1996, the Commissioner's Instructions were amended to include the following direction — 'Make a notebook entry recording the reason for a computer access unless it is abundantly clear from departmental records [that] the access was lawful.'

In its submissions to this Inquiry, the NSW Police Service indicated that audit and evaluation results demonstrated a high degree of compliance with personnel recording 'reason for access' in their official notebook or duty book, and that 'Officers appear to accept responsibility to record access as part of their job and insurance against allegations of misuse of information' (NSW Police Service Submission 2000, p. 13). The NSW Police Service is also working toward electronic capture of reasons for transactions and, in the interim, has made the demands of recording less by allowing:

- large jobs to be processed as a 'batch job' requiring only one entry to be recorded
- recording of a single entry in their official notebook, duty book or terminal register when a series of transactions are related
- country radio operators and, where appropriate, general support officers to record reasons in terminal registers and logs
- audio tape-recording and radio log registers, using infringement notices or information reports as reason for transaction.

The following indicates the view of the NSW Police Service on the functionality of a 'reason for transaction' requirement:

Chairperson: It seems to me that an audit process would be much less effective if you weren't able to cross check against a reason for access.

Commander Brammer: Oh, for sure. It would be useless, basically, I think ... I think

you've got to have that cross-checking ability. (CJC unpub, pp. 757–58)

Lessons learnt from the NSW experience

The NSW experience indicates that the NSW Police Service recognises the need to implement a system that allows effective auditing and investigation to be undertaken. In both its written and its oral submissions, the NSW Police Service conceded that requiring members to record reasons for transactions consumed more time. However, it argued that there is a clear need to make individual officers accountable and responsible if the confidentiality of information recorded on the computer mainframe system was to be maintained. It is also important to note the futility of partially implementing an information-security strategy. If an information-security issue is to be tackled, it must be done in a comprehensive way to ensure that any foreseeable 'gaps' are removed and/or minimised.

The Queensland case

As in New South Wales, there has been ongoing debate on the issue of 'reason for transaction'. In 1994, the then Chairperson of the CJC, Mr R S O'Regan QC, wrote to the Commissioner of Police stating that the continuing high number of allegations of misuse of confidential information indicated that preventative action needed to be taken by the QPS. Mr O'Regan suggested²⁰ that a 'reason for transaction' field would serve as a memory prompt for officers when audits were performed and would prevent them from telling investigators that they were simply unable to recall why they made the check in question. Mr O'Regan stated that investigations of allegations of this nature were being frustrated by such responses, which could not be shown to be false when, as is often the case, officers are required to make numerous searches of the QPS databases for legitimate purposes. Mr O'Regan went on to state that, while he accepted that no system could guarantee that abuses of that kind would not occur, any improvement should be welcomed.

The Commissioner replied that an additional field to record reasons for computer access has merit as a deterrent and could also be a useful investigative tool if implemented properly. However, the Commissioner also pointed out that if the overhead in system-processing and user-response rate was greatly degraded, then a decision would need to be made as to which direction posed a greater risk to the QPS. The Commissioner advised that, until further information on the issue was collected, it would be inappropriate for the QPS to introduce a 'reason for transaction' requirement.

On 31 October 1994 the Chairperson wrote to the Commissioner stating the CJC's interest in the security aspects of the QPS's redevelopment of its information systems. The letter responded to the QPS's decision on the 'reason for transaction' field in the following way:

While coded reasons [for transactions] may be questioned for their usefulness in the Courts where the standard of proof is 'beyond reasonable doubt', such information would be very relevant in Queensland where the standard of proof in Misconduct Tribunals is 'on the balance of probabilities' and useful in the open disciplinary processes used in Queensland.

Also in this letter the Chairperson commented 'that some alarming circumstances have been uncovered through the investigation of complaints to the Commission, including identification of officers in sensitive positions providing information to private investigators and commercial agents'.

On 13 December 1994 the CJC was advised that, as part of the new computer-access procedures, the new QPS computer system (called POLARIS) would provide the ability to record a reason against each inquiry made on the system. The QPS also released an internal report entitled **Requirement Analysis Specification for the Application Auditing Service** (30 November 1994), which stated that the 'user interface should include a provision to extract the reason for access from the user which should be included in the audit trail'. It was also acknowledged that such a system could be cumbersome to implement and that the 'final design of the reason function would be determined in concert with POLARIS users and representatives from the CJC and Inspectorate to ensure that it would be helpful for investigative purposes but be a minimal overhead for users'.

On 17 January 1997 the CJC received a letter stating that there were serious concerns with the implementation of the 'reason for transaction' requirement. This concern was raised just before POLARIS Release 1 was activated at the end of October 1996 and, as a result, implementation had been deferred. That letter also invited comments for consideration for the next meeting of the POLARIS Release 1 Project Board.

On 7 April 1997, the CJC wrote stating its position and the views put forward by the then Chief Superintendent of the Commissioner's Inspectorate, Mr Jefferies. Mr Jefferies had given the following reasons for the necessity to supply reasons when using the POLARIS system:

- To improve the auditing facility that is presently available;
- To reduce the amount of time necessary to complete an investigation;
- To make all users of POLARIS accountable for their actions;
- The expected implementation of Privacy legislation in Queensland later this year will require the service to be accountable for personal information that is accessed;
- Other Police Services within Australia have found it necessary to implement policies and systems which make users of police information systems accountable for all information.

The CJC did not hear further from the QPS until it received a memorandum dated 19 May 1997 stating that the POLARIS Release 1 Project Board had considered submissions in relation to the introduction of a 'reason for transaction' field and on 17 March 1997 had concluded that the facility would not add value to the POLARIS audit trail and that the investigator would still need to prove that the reason given was false. The Board did agree, however, that this requirement may need to be reconsidered when sensitive information such as intelligence data are recorded on the system in future releases. The memorandum indicated that this recommendation had been approved by the Deputy Commissioner. It was noted in later correspondence that the POLARIS Release 1 Project Board had made its decision and recommendation before it had received the CJC submission of 7 April 1997.

On 20 August 1997 the Chairperson again wrote to the Commissioner requesting that serious consideration be given to issuing a policy directive to the POLARIS 1 Release Management Board that 'it introduce a facility to allow the recording of a "reason for transaction" when accessing POLARIS'. It was commented that:

The Commission still receives many complaints alleging misuse of confidential information. Also, in recent times, particularly since the inception of Project Shield,²¹ there have been a number of occasions in which surveillance vehicles have been compromised, in that computer checks have been carried out on covert vehicles. It is not possible with the current audit system to ascertain whether the inquiries made were routine traffic inquiries or something more sinister.

The letter emphasised that the types of checks being observed had the potential not only to compromise current and future operations but also to place at risk the safety of operatives. It was

to become apparent that this type of improper use of QPS computer systems would develop into a serious problem for Project Shield.

The Commissioner wrote back to the Chairperson on 18 September 1997:

... as the full impact of the 'reason for transaction' facility became apparent on the usability of the system and what the facility would and would not provide in terms of system security, the Polaris User Team developed reservations as to the desirability of including the facility in Release 1. These reservations were based on the following matters:

- The facility would introduce another level of bureaucracy in the usage of the system and this had the potential to adversely effect the usability and acceptance of Polaris;
- It was expected that in a short space of time, users would enter a routine, and legitimate 'reason for transaction' that in the end would subsequently offer little to either investigators or the users as to the real reason for access;
- The onus would still rest with investigators to disprove the accuracy of the entry in the 'reason for transaction' field during any investigations;
- A very extensive security system had been developed for Polaris that enabled investigators to replay transactions undertaken by users.

However, the Commissioner did indicate that he believed it to be appropriate that the issue should continue to be reviewed in conjunction with future releases of POLARIS.

In October 1997 the CJC released its report resulting from Project Shield, entitled *Police and Drugs: A Report of an Investigation of Cases Involving Queensland Police Officers*. The report, prepared by the Honourable W J Carter QC, included many examples of police officers and civilians accessing computer databases for purposes unrelated to police work. When investigators attempted to determine the reason for the checks, 'those persons who made the checks were, not surprisingly, unable or unwilling to say on whose behalf the checks were made and for what purpose' (CJC 1997a, p. 60). Because of these investigative difficulties and the ease with which inappropriate inquiries could be made anonymously and without explanation, it was recommended that a computer security screen ('reason for access') be introduced on the

QPS computer (CJC 1997a, Recommendation 7(i)).

The subsequent CJC report **Police and Drugs — A Follow-up Report** (1999a) observed that the recommendation regarding the use of a ‘security screen’ had not been adopted by the QPS. As noted in the report, the (then) Deputy Commissioner of Police wrote to the CJC indicating that the QPS ‘would not be adopting this recommendation because it is not considered the additional field is of sufficient value to justify its inclusion’. He also adopted the QPS’s previous response to the proposal in the letter dated 18 September 1997 (quoted above).

Notwithstanding the reasons put forward by the QPS to justify their stance against the CJC’s recommendation, the CJC expressed the view that the benefits associated with the introduction of a security screen exceeded the costs associated with its introduction. Appendix P has an excerpt from the report outlining the CJC’s comment on the QPS’s decision to reject a ‘reason for transaction’ field.

It should be mentioned here that, during this Public Inquiry, the QPS did indicate that their new computer system, which will allow direct access to the criminal history of individuals, will require users to nominate the reason for viewing criminal-history information. The user-ID and reason for viewing will be recorded in the computer system’s audit-trail holdings. Any printed documents from the system will have a ‘water mark’ showing the user-ID and organisational unit. In its submission, the QPS indicated that it ‘would need to evaluate its [reason for transaction requirement] cost-effectiveness before considering any expansion of the system’ (QPS submission 2000, p. 21).

The QPS also argued that the ‘reason for transaction’ requirement was a justifiable and reasonable control to implement for this particular system because of the nature of the information and the risk of misuse. The CJC does not consider criminal-charge history or personal information (e.g. address and phone number) to be any less sensitive than criminal history. Criminal-charge information is potentially more sensitive because it may be misinterpreted as the same as criminal history and remains on the QPS systems even if the individual is found not guilty.

The CJC appreciates that effective information security is much broader than a single feature such as the ‘reason for transaction’ requirement; however, this requirement is one critical feature of an information-security approach to dealing with the type of misconduct revealed by this

Inquiry. The issue of concern is that, despite the implementation of many information-security measures, investigations and audits on access to QPS computer systems cannot be conducted effectively without the ability to cross-check against a ‘reason for access’ record. This was evident in this Inquiry, previous CJC inquiries and investigations, and inquiries and investigations conducted in other jurisdictions.

The purpose of a requirement to record reason for transaction is not only to investigate officers suspected of improperly accessing computer systems, but also to provide an effective means of exonerating those who have been wrongly accused of such misconduct. It is unrealistic to expect officers to recall the reason for a transaction that they conducted some time ago. The lack of a requirement to record reasons for transactions does not serve honest QPS members well and only provides a convenient defence for those involved in misconduct, official misconduct and corruption.

In its submission to the Inquiry, the QPS raised a number of objections to a ‘reason for transaction’ requirement, and each is addressed as follows:

- **A free text field or screen for ‘reason for access’ cannot guarantee a satisfactory or reasonable explanation of activity undertaken** — In recommending the ‘reason for transaction’ field, the CJC did not argue that it is a fool-proof prevention measure; no single prevention measure ever is. An effective prevention strategy combines a range of complementary initiatives aimed at minimising the occurrence of, and opportunity for, improper conduct. A ‘reason for transaction’ requirement will raise user awareness and provide a defence for members wrongly accused of inappropriate access, and is essential for effective investigation and audit. It is true that recalcitrant members may well enter false reasons; however, manufactured reasons will be easier to investigate and disprove than no reason at all. This of itself will serve to identify suspect members and facilitate an appropriate managerial response to the conduct of such officers (e.g. increased level of supervision). Prevention initiatives, like legislation, orders and policies, should not be cast aside because they may not be adhered to by all members. Similarly, the CJC does not consider the fact that some members may enter false reasons for transactions as a sufficient argument to discount this initiative.
- **The cost of such an initiative would be high in relation to any possible benefit** — This submission has not been supported by any

meaningful costings. The QPS has also been dismissive of the hidden costs of the present system. There are substantial costs in conducting the investigations into this type of misconduct undertaken by both the ESC and the CJC. Many of these investigations fail to achieve an effective result because members do not have to account for their computer transactions. This Inquiry alone has cost thousands of labour hours for both the CJC and QPS over the last two years. This does not include the cost to the QPS for the time spent by the subject officers during working hours to conduct searches unrelated to their duties as a police officer. It must also be recognised that the costs of requiring a reason for transaction are off-set by the productivity gains that flow from information systems permitting immediate access to information that previously would have taken days or weeks to obtain and would have required significant labour hours to process. Clearly it is extremely difficult to make a fair and accurate estimate of cost-benefit given the above issues and the fact that the extent of the problem is unknown.

Certainly, the implementation of a 'reason for transaction' requirement can be very costly if done strictly through IT functions; however, as seen in the NSW Police Service, the combination of different media to record reasons for transactions can reduce financial cost significantly. Different systems for recording transaction can be used. For example, for more sensitive information/records, a mandatory 'reason for transaction' field built into the computer system may be most appropriate, whereas for other information/records a written record in the police notebook or some other register may be adequate. Similarly, the creation of official police records may be sufficient (e.g. check on vehicle registration verified by the issue of a speeding ticket). The decision as to the medium for recording reasons for transactions is a matter for the QPS to determine.

- It will constitute a minor inconvenience and irritation to the vast majority of honest officers and may discourage officers from using their initiative to access information, particularly if the reason is just a hunch — The QPS's adoption of the risk-assessment and risk-management philosophy has at times caused inconvenience and irritation, as new systems are bound to do. No doubt members have felt inconvenienced when required to enter information into an index or subjected to an inspection. However, these innovations have eventually been accepted by members

as necessary if the Service is to discharge its responsibility of ensuring that orders, policies and procedures are complied with. As noted in the submission of the NSW Police Service, members have moved from feeling inconvenienced to accepting the requirement to record a reason for transaction. The concern that members may be discouraged from using their initiative is better met by education and training rather than compromising information-security strategies. Furthermore, if members are confident of their reasons for using the computer system, even if based on a hunch, it should make no difference that a reason for transaction is required.

- If it is to be used it should be restricted to those systems which have particularly sensitive information and where there is potential serious risk if the information were to be handled inappropriately — In its written submission (2000, p. 21), the QPS indicated that one area where a 'reason for access' screen is necessary is in the new system that gives officers access to criminal-history records. The CJC considers that criminal history, which is publicly available at the time of the court case, is of the same classification and risk level as criminal-charge histories and personal information that can be used to locate a person. If the QPS considers it a necessary security measure to record reasons for access to criminal-history records, the same necessity applies to other in-confidence information.

Like the Office of the NSW Ombudsman, the CJC firmly believes that the QPS should implement a system of accountability for authorised users accessing the QPS computer systems. There does not appear to be any effective alternative to the requirement of having members record their reasons for transactions. The method and program of implementation are matters for the QPS and must be considered as part of the strategic planning process. It is for the QPS to determine when mandatory computer fields are preferred over a written record. The QPS should also ensure that, where a search is conducted on behalf of someone else, appropriate systems are in place to identify the person who requested the search and the reasons for that search.

RECOMMENDATION 6.11 — REASON FOR TRANSACTION

6.11.1 That the Queensland Police Service order that all members must record a reason for access for each transaction made on the corporate/mainframe computer systems, either through mandatory computer entry, police

notebook entry, or some other systematic documentation process, except where:

- a series of transactions are logically linked, in which case a single reason for the multiple transactions will afford an appropriate level of accountability
- where other official police documents provide evidence of an appropriate reason for the transaction
- where the duties of an officer require an unusually high number of transactions in relation to information that would routinely be accessed (e.g. a traffic police officer performing vehicle-registration checks).

The last proviso should not apply to those members accessing sensitive information, such as intelligence databases.

6.11.2 That, where transactions are conducted on behalf of another member, the requesting member be required to record a reason for the request through mandatory computer entry, police notebook entry, or some other systematic documentation process.

6.11.3 That, where transactions are conducted on behalf of another member, the person conducting them asks the requesting member the reason for their request and their name, and records that information through mandatory computer entry, police notebook entry, or some other systematic documentation process.

INFORMATION-SECURITY AWARENESS AND INDIVIDUAL ACCOUNTABILITY

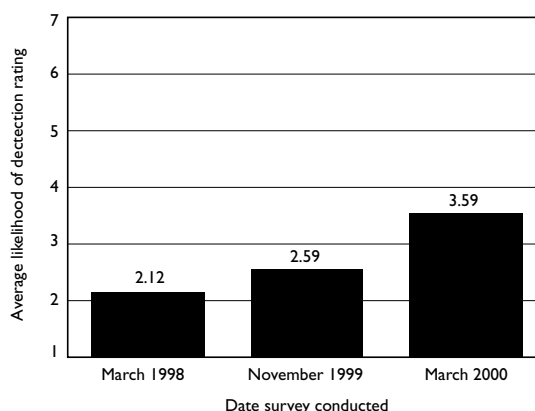
As has been well documented within the literature, awareness and education are not the same. Raising awareness involves firstly capturing attention and then following through with reminders. Reminders may take many forms, such as posters or computer warning screens. In the case of information security, the goal of an awareness strategy is to have members aware of information-security issues in their day-to-day actions — the desirable outcome is members who make informed and ethical decisions about their use of, and access to, QPS computer systems.

The public hearing of the CJC raised awareness of the issue, particularly among the FYCs surveyed by the CJC (discussed below). It also resulted in an increase in the number of complaints of improper disclosure of information. This may be because members of the community now realise that they can make complaints of this nature to the CJC.

The surveys that the CJC administers to QPS FYCs to ascertain their views on ethical conduct and the complaints and discipline process indicate that since the Public Inquiry there has been a notable shift in perceptions of the likelihood of an officer's being detected when performing an unauthorised check on a motor-vehicle registration (the surveys are explained in detail on page 64–65). There is no reason to assume that this shift in perception is restricted to FYCs, for the majority of police officers are also likely to have had their awareness of this issue heightened, given the media attention generated during this Inquiry.

As shown in figure 6.3, FYCs surveyed in March 2000, very soon after the closing of the public hearing on 8 March 2000, were more likely to consider that such behaviour would be detected than were officers surveyed in 1998 and 1999.

Figure 6.3 — Perceived likelihood of being detected while conducting an unauthorised vehicle-registration check



Source: Research and Prevention Division, CJC

Notes:

1. Rating scale is 1 to 7, with 1 being 'not at all likely' and 7 being 'very likely'.
2. Subjects were First-Year Constables surveyed in 1998 and 1999.
3. N size for each group ranged from 113 to 155.

Aside from the publicity generated by the Inquiry, no processes or systems for detection or investigation have changed. The change in perception may be due to increased awareness that the inappropriate use of computer systems is a serious matter that may be investigated.

It is necessary for the QPS to develop strategies to raise awareness, and an effective first step would be a notice from the Commissioner of Police stating (for example):

- why this Inquiry occurred
- the outcome of the Inquiry in terms of the sanctions imposed on the officers

- the position of the QPS on information security and the strategies to be implemented in future to deal with the problem
- that the use of the computer system for personal or other non-official reasons will not be tolerated
- that members who cannot demonstrate that their access was for official police work may face disciplinary or criminal charges.

The QPS also uses a warning screen that appears each time the user logs onto POLARIS (appendix N) and QPS System (appendix O). Both screens list the conditions of access to, and use of, the computer system and quite clearly state: 'You are NOT authorised to access information for personal reasons.' The difficulty is that users do not read the warning screen when logging on. The QPS could implement an electronic and mandatory sign-off on the warning each time the

Figure 6.4 — Statement of Responsibility used by the NSW Police Service

STATEMENT OF RESPONSIBILITY

NSW POLICE SERVICE

INFORMATION AND INFORMATION SYSTEMS

All employees of the NSW Police Service are to abide by the Service's "Code of Best Practice and guidelines for Management of Information and Information Systems." and are accountable to the Commissioner to:

- (a) comply with all legal prescriptions regarding the handling of information.
- (b) protect information stored in both documentary and computer systems.
- (c) treat all information coming to their attention as strictly confidential.
- (d) not communicate in any way information regarding police business without proper authority.
- (d) report any breaches of security to their Commander or the Commander, Office of Professional Responsibility.

All employees of the NSW Police Service are responsible for the security of information on the Service's computer system. Users must understand and comply with the following protection requirements:

- (1) Access computers and computer systems is authorised for the performance of duties only. Information is not to be put to any personal use.
- (2) Access to sensitive information is logged. Any users attempting unauthorised access will be called to account by their Commanders and the Assistant Commissioner, Professional Responsibility.
- (3) Unauthorised software, including computer games, must not be loaded onto Police Service microcomputer terminals or personal computers.
- (4) Passwords must be memorised and kept confidential. Do not display them on or near a terminal. Never disclose passwords even to a supervisor or fellow worker who may seem to have a reasonable request.
- (5) Users are required to change their password once a month. Choose a password which is easy to remember but not easily guessed. Passwords must be at least six characters in length.
- (6) Users must not leave a logged on terminal unattended. This will prevent another person from accessing information which would in turn be logged against you as a user.
- (7) Users will be held accountable for activities which take place under their passwords. If you suspect another person has knowledge of your password you must change it. Report any suspected violations to Commanders.
- (8) Appropriate sanctions under the Police Service Act, Public Sector Management Act and Crimes Act shall be applied for misuse and breaches of security.

I have read the Statement of Responsibility and as a user understand my obligations.

Name/Number/Command _____

Signature _____ Date _____

user enters the system. However, there are arguably better strategies, such as those recommended throughout this report, to raise the general awareness of the user.

The QPS currently requires civilian members to sign a confidentiality agreement in relation to computer access and use (see page 51) before being permitted to begin using the computer system. This agreement is similar to the Statement of Responsibility (figure 6.4), which all members of the NSW Police Service are required to sign at the commencement of their employment.

The CJC considers that it should be compulsory for all members of the QPS to agree to and sign a confidentiality acknowledgment. The purpose of the acknowledgment is to raise awareness, improve accountability and emphasise the importance of information security. The acknowledgment makes users responsible for transactions made under their user-ID and places the onus on them to demonstrate that their transactions were for official police work.

As part of a strategy to emphasise individual responsibility and accountability in the use of the computer system, all members of the QPS should be required to sign an acknowledgment that they:

- agree to the information-security policies (e.g. 'Never disclose your password', 'Never leave an open terminal unattended', 'Always record a reason for transaction except where exemptions are made under QPS policy') that are listed in the contract/agreement
- have read and understood the legislation, orders, policies and procedures relating to information security within the QPS
- will abide by those provisions and understand that if they breach the agreement/contract they will be disciplined or dismissed.

Provisions must also be made to prevent members from signing the acknowledgment without reading it. The most suitable mechanism is to have a supervisor/manager witness the signing and also sign the acknowledgment, stating that the member has demonstrated that he/she has read the acknowledgment and fully understood it. Where a supervisor/manager is not satisfied that the member has the necessary understanding and knowledge of the legislation, orders, policies and procedures relating to computer information security, access should not be granted until the member completes appropriate training and education on information security.

It is important that the acknowledgment be

renewed from time to time to ensure that members do not forget their obligations regarding information security. The nature of policing is such that many employees, particularly police officers, may stay with the Service for their entire career. Employees need to be reminded of their obligations throughout their career and advised of changes to information-security policies and practices. As more and more information becomes available to members on the computer systems, the QPS will need to be vigilant in renewing its members' agreement to adhere to the information-security policies.

It is impractical to suggest that the QPS should have all employees renew their acknowledgment each year. It will be administratively easier to have this renewal process integrated into an already existing process. One such process is the application to entitle the individual to be an authorised user of the QPS computer systems.

Members are required to apply for access, or renewal of access, to computer corporate/mainframe systems to the ISS. As part of the application process, it would be effective to have members, and their respective supervisors/managers, sign and renew their acknowledgment. Such a requirement would be timely, given that the member is about to be granted access to a computer system/database that contains confidential information. It also satisfies the ISS requirement that the applicant be suitably aware of, and trained in, information security as it relates to computer use.

RECOMMENDATION 6.12 — RAISING AWARENESS OF INFORMATION SECURITY AND INDIVIDUAL ACCOUNTABILITY

6.12.1 That, in response to this report, the Commissioner of Police issue a notice to all members, addressing the issues arising from this Inquiry, areas of concern and policy developments in respect of information security.

6.12.2 That the Queensland Police Service require all members to sign an acknowledgment stating that they:

- agree to the information-security policies as specified
- fully understand that the QPS computer system is not for personal use and, therefore should only ever be accessed and used in the performance of official police work

- have read the legislation and will abide by the legislation, orders, policy and procedural rules and guidelines on computer use and access, and release of information
- understand that a breach of the terms of the contract/agreement will result in criminal and/or disciplinary action and possible dismissal.

To ensure that no significant administrative burden is placed on the QPS, implementation should be progressive and be applicable to all new recruits from January 2001.

6.12.3 That a supervisor or manager witness the signing of the acknowledgment, and also attest that the member has demonstrated that he/she has read the contract/agreement and fully understands its content.

6.12.4 That, where a supervisor or manager is not satisfied that a member has the necessary understanding of legislation, orders, policies and procedures relating to security of computer information, access should not be granted until the member completes appropriate training and education.

6.12.5 That all members be required to resign their acknowledgment when they request new, changed or renewed access to a mainframe/corporate system or database.

TRAINING AND EDUCATION IN INFORMATION SECURITY

The training provided to recruits in the PROVE and POCC programs is comprehensive with regard to computer use and information security (described on pages 49–50). However, the training programs for more senior members of the QPS concentrate more on ethics training than information security and effective supervisory practices.

In addition, the preliminary findings of a recent survey on policing and IT (Chan, J. et al. forthcoming) within the QPS show that as officers progress in rank they spend less time using computers/databases, are more likely to see themselves as incompetent at using IT and are less likely to receive computer training. The preliminary findings demonstrate the need to ensure that senior officers are receiving the necessary training. If supervisors are to supervise their subordinates effectively in computer use, they must be proficient at using and understanding the systems themselves and, arguably, must be better trained in information security. Supervisors must also understand, and be able to apply, the principles of risk management. The QPS has adopted risk-based

assessment as a critical management function. It is important that supervisors can apply risk-management principles in the context of information security.

In its written submission, the QPS stated that:

The strongest protection [for information security] comes from education and training programs that emphasise the responsibility members have for maintaining secure systems and processes. The Service will examine its training programs in light of any outcomes of the present inquiry, to identify means of re-emphasising the responsibilities of staff in relation to the information they have access to. (QPS submission 2000, p. 26)

It should be noted that the QPS did not claim that training and education were the only components of a program aimed at preserving information security, but that it was the strongest component.

The CJC does not agree that the strongest protection comes from education and training programs. It is difficult to ascertain which components of a strategic approach provide the greatest prevention and deterrent effect. The CJC is of the view that it is the combined effect of the full collection of complementary initiatives, policies, procedures and practices that affords the strongest protection and provides the necessary prevention and deterrent effects. The QPS must be careful not to place too much reliance on training and education to ensure compliance with information-security orders, policies and procedures. As was observed during the Inquiry, one officer who had received extensive training in computer use and information security conducted over 300 inappropriate checks on the computer system. This officer quite clearly knew of his obligations and in fact had written an assignment citing many examples of inappropriate use.

Nevertheless, training and education are important components of an overall information-security strategy. As computers are increasingly relied upon in police work, the training in computer use and information security must form part of the training and education programs for members later in their career. The QPS computer system is continually evolving, and therefore requires continuity in training for all ranks and positions in the Service. As the systems develop, so should the information security policies. Managers, in particular, should be familiar with the changes and able to implement supervisory and risk-management processes to ensure compliance.

The QPS indicated in its submission that it was developing a CAP (Competency Acquisition Program) module that was specifically concerned with computer use and information security. The CJC urges the QPS to complete the module, as it is important to provide further training in the area for civilian members of the QPS and remedial training for those members who are assessed as in need of it.

RECOMMENDATION 6.13 — EXTENDING INFORMATION SECURITY

6.13.1 That the Queensland Police Service incorporate, in higher education and training programs, particularly those catering for supervisors and managers, training sessions/modules on computer use, information security and supervision of computer use by subordinates.

6.13.2 That the Queensland Police Service educate managers and supervisors on the application of the principles of risk management to develop processes for the effective monitoring and supervision of subordinate staff in the use of, and access to, the police computer system.

6.13.3 That the Queensland Police Service complete the development of the Competency Acquisition Program module on computer use and information security.

CONCLUSION

Management of information security is becoming an increasingly high priority for organisations. This is not surprising, given that information is well recognised as a valuable asset to the organisation. The advent of information technology has resulted in significant increases in the efficiency of information systems, facilitated the development of open communication systems and provided many individuals with immediate access to information that allows them to perform their duties more effectively.

With these rapid advances has come greater risk. This risk has been made even greater because of the lag in technology designed to mitigate those risks and the delay in organisations' recognising the need to have management of strong information security. In assessing the QPS system for managing information security, all of the following were considered:

- the Australian and New Zealand Standard on Information Security Management (AS/NZS 4444.1:1999) in combination with the review of current literature in best practice

- the issues raised through public submissions and presentation of evidence
- the lessons to be learnt from other jurisdictions, particularly the NSW Police Service
- the final comments and submission made by the QPS.

In this chapter, recommendations have been made that represent both an organisational and a technological response to the issues raised. A significant number of recommendations have been made to 'close any gaps' in policy and procedure (e.g. policy to prohibit leaving open computer terminals unattended, proper disposal of paper copies of in-confidence material and mandatory recording of reasons for transactions).

It has also been recommended that the location of the ISS be reviewed, giving consideration to its placement within the ESC. Technological recommendations for the development of features such as 'alert' monitoring to improve detection systems have also been made. Finally, it has been recommended that the QPS commence a program of systematic and ongoing internal audit on access and use of QPS computer systems. Such a program should have both random and targeted components. This will allow the Service to be proactive in its monitoring of this type of misconduct.

THE MARKET FOR INFORMATION

In 1992 the ICAC released its report on the unauthorised release of government information after a two-year Inquiry. Evidence was heard from approximately 466 witnesses over a total of 168 hearing days. The ICAC found that the principal participants in the illicit information trade in NSW were:

1. Police, Roads and Traffic Authority officers and other New South Wales public officials, who have corruptly sold confidential information entrusted to their care.
2. Insurance companies, banks and other financial institutions, which have provided a ready market for that information, and have been major contributors to the thriving trade which developed.
3. Private inquiry and commercial agents, who have acted as brokers and retailers, providing the necessary link between anxious buyer and ready seller. (p. 3)

Not surprisingly, observations made during this Inquiry indicate that the market for information in Queensland is very similar. However, this Inquiry was initiated in response to allegations against members of the QPS and so did not extend to other areas of the public sector.

This chapter aims to describe the nature of the information market and why there is a demand for illicit information. The first section of the chapter makes a number of observations about the market for information. The second section details the systems currently in place in Queensland for obtaining information held by government agencies. Finally, the issue of whether restricted information should be made available to solicitors, lawyers, mercantile agents and private investigators is discussed.

OBSERVATIONS MADE DURING THIS INQUIRY

A number of observations can be made in respect of the nature and operation of the information market.

The end-users of information

Evidence before the CJC showed that the end-user of the information, that is, the people or companies who employed the private investigator to obtain illicit information, were:

- insurance companies
- solicitors
- leasing companies
- a range of private-sector organisations (e.g. a real-estate agent)
- other private investigation firms
- individuals.

It is worth noting here the comments and results of the ICAC Inquiry (1992a) regarding end-users. Many of the end-users and their supervisors were called to give evidence at the ICAC Inquiry. It was submitted by a number of corporations that they should not be held responsible for the conduct of their officers who had made requests to private investigators to obtain illicit information. They argued that it was 'the individual officers, and not the banks or insurance or finance companies, that had supported the illicit trade, and had contributed to the corrupt conduct on which it was based' (p. 134). Similarly, a number of solicitors maintained that it was in order for them to purchase confidential information from private investigators 'without concerning themselves with the means by which it was obtained' (p. 134).

Commissioner Temby, who authored the public report, commented that such improper conduct occurred because of the 'wilful blindness' of senior officers, who did not want to know, and 'of the boardroom wanting to remain untouched by the grime of the workroom' (p. 135). It was further argued that 'reasonable principles must be established to prevent corporations from hiding behind employees who are allowed, encouraged or even required to engage in criminal conduct on their behalf' (p. 146). The report also highlighted the dilemma for lawyers of balancing the desire to assist their clients with their duty to

uphold the law. It became apparent during the ICAC Inquiry that different sections of the legal profession held vastly different views on the practice of obtaining illicit information and that this was a matter that needed serious attention.

The CJC, like the ICAC, does not have jurisdiction over the operation of private-sector businesses and corporations. However, the private sector was an end-user that paid for the confidential information that was improperly released. For this reason, the CJC cannot ignore the operation of private-sector organisations where it contributes to the prevalence of misconduct, official misconduct and corruption within the public sector. In chapter 9 ('Information Protection and the Law') the CJC recommends the creation of offences that prohibit individuals, including corporations, from obtaining or trying to obtain confidential information in government records where it concerns other people, however it is held.

Reasons for seeking information

During this Inquiry it was noted that confidential information was sought for a range of reasons (table 7.1). The amount charged or the budget allocated for the provision of information and services is also listed.

Requesting illicit information

Requests for criminal histories were usually made

in relation to a court matter, whereas requests for driver's licence details and vehicle registration checks were usually for the purpose of locating an individual. Requests for 'background inquiries' were frequently met with reports that included driver's licence details and criminal-offence and traffic history. This suggested that 'background inquiries' generally included that type of information as a matter of course.

Other requests for information were less subtle — for example, 'obtain criminal history' or 'obtain traffic history'. Figure 7.1 is a fax seized, during the Inquiry, directly requesting driver's licence details.

QPS computer audit trails show that one of the subject police officers conducted a search (query driver's licence) on the name given in the above fax on 5 September 1996. On 6 September 1996 the client was sent the letter shown in figure 7.2 from the private investigator.

It is of concern that private-sector organisations made direct requests for information that was not lawfully obtainable. This may have been out of ignorance, or without regard for the means by which the information was obtained, or, more disturbingly, knowing that those who were asked to obtain the information would have to break the law to do so.

Table 7.1 — Reasons and financial charges for information searches observed during this Inquiry

A client of a legal firm was owed money for services rendered but the debtor had moved and could not be located through normal means — the firm indicated that the investigator had a budget of \$75.

An insurance company needed to issue an 'intention to sue' notice for monies owing from a motor-vehicle accident but were unable to locate the person concerned — the fee charged and paid was not specified.

A legal firm had obtained a Magistrates Court judgment against two people who had moved and could not be located through normal means — the firm indicated that the investigator should not exceed a budget of \$100 without contacting them.

An engineering company wanted to 'check out' a person whom the company had entrusted 'with the safety of our properties at [address] and [address]' — the private investigator charged \$145 to conduct the inquiries and prepare the report.

A legal firm could not locate a person whom they wished to serve with a District Court Plaintiff and forwarded the court documents to the private investigator to locate and serve — the private investigator indicated that the fee to locate and serve was \$160.

A legal firm was instructed by their client to locate his wife and daughter so he that could have contact with his daughter, whom he had not seen for three or four years — the firm indicated that the private investigator should not exceed a budget of \$100 in the preliminary inquiries.

A client of an investigations company needed to locate a witness to an accident because the accident victim was suing the client for negligence — the private investigator charged \$130 to conduct the inquiries.

Figure 7.1 — Seized fax showing request for driver's licence details

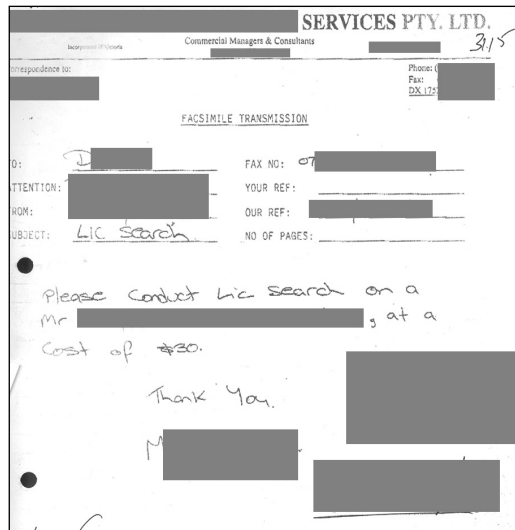
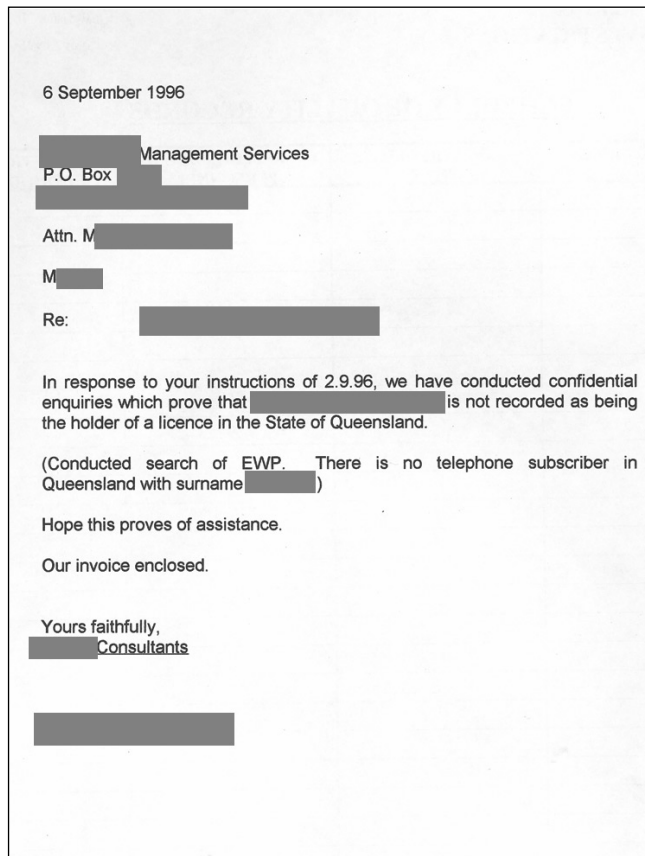


Figure 7.2 — Seized letter showing outcome of driver's licence check



Industry fees for information

During the Inquiry, the cleaner at the Nerang station (N1) gave evidence concerning the fees he had charged for information:

Counsel Assisting: Was there a certain amount of money that you would receive for certain types of information?

N1: To the best of my recollection anything between 10 or \$15 for a licence or registration check and anything from 30 up to 40 or \$50 for more detailed or traffic or charge information.

Counsel Assisting: Criminal charge information?

N1: Yes. (CJC unpub., p. 224)

These charges were similar to those recorded on documents seized from one private investigator (N2) — see figures 7.3 and 7.4.

Figure 7.3 — Seized document showing fees for different types of ‘background inquiries’

Service	Quantity	Unit Price	Total Price
To conduct enquiries - personal searches	x 1	110.00	110.00
company searches - extracts	27	5.00	135.00
credit searches - personal	x 3	21.00	63.00
company	x 3	14.00	42.00
property searches	—	48.00	48.00
licence/rego	20	1.25	25.00
criminal	50	0.80	40.00
telephone	10	10.00	100.00
electoral roll	10	1.00	10.00
titles office	20	1.00	20.00
confidential enquiries	—	20.00	20.00
interview	5	11.00	55.00
Type report	2.5 x 55	135.00	135.00
Total			1129.00

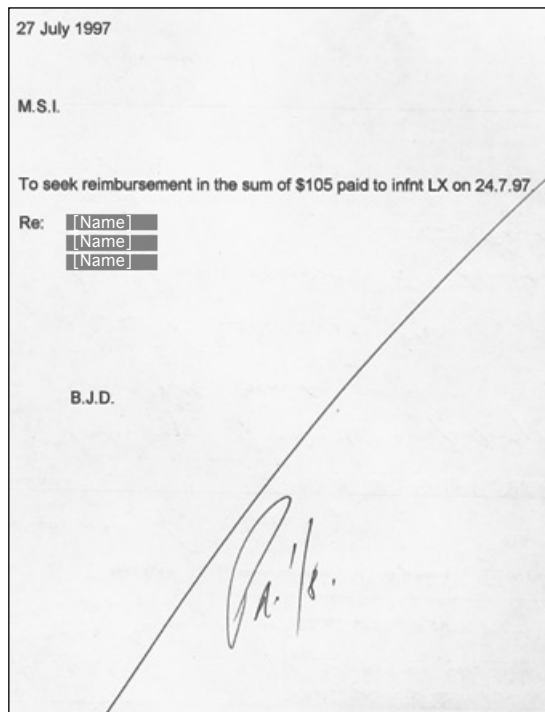
Handwritten notes on the document include: "2 x 55 = 110.00", "Follow", "7 x 55.00", "365.00", and "1129.00".

Similarly, an invoice seized by the CJC evidenced that N2 paid informant LX approximately \$35 for each person on whom he provided information.

CURRENT SYSTEMS AND PROVISIONS FOR ACCESSING GOVERNMENT INFORMATION

Within Queensland there are three ways, subject to certain qualifying conditions, for businesses and individuals to access the type of information that was sought by the end-users identified during this investigation. These are:

Figure 7.4 – Seized invoice showing fees paid to informant LX for providing information on three individuals



Note: Computer audit trails presented in evidence at the Inquiry showed that one or more of the subject officers had accessed the police computer records on the three names given in the invoice. All of the accesses occurred before to the date of the invoice.

- CITEC CONFIRM
- QPS PIC
- Queensland Transport.

CITEC CONFIRM

CITEC is a commercial business unit of Queensland Government and is part of the Department of Communication and Information, Local Government and Planning. CITEC specialises in IT and communications and has four main areas: IT Services, Network Services, Business Systems and Information Services. CITEC CONFIRM, which is located within Information Services, provides access for businesses and individuals to certain types of government-held information. CITEC CONFIRM acts as a brokerage information service that provides a ‘one-stop-shop’ for legal firms, insurance companies, banking and financial institutions, government agencies, search agents, debt collectors and private investigators. The databases that are available are shown in table 7.2 on page 81.

Prospective users can register for access to all databases through the CITEC CONFIRM web-site. The information held on the unrestricted databases is publicly available and can be

Table 7.2 — Databases available through CITEC CONFIRM

COMMODITY	DATABASES
Corporate Searches — Australian Securities and Investments Commission	<ul style="list-style-type: none"> • All State Business Names • Directors • Company Extracts • Business Owner Search • Organisational Extracts • Australian Securities and Investments • Commission Alert • Company History
Corporate Reports — Australian Corporate Reporting	<ul style="list-style-type: none"> • Credit Reports • Analytical Reports • Contractor Reports • Building Industry Reports • Trade Reports • Adverse Information
Bankruptcy Searches	<ul style="list-style-type: none"> • National Personal Bankruptcy
Property Searches	<ul style="list-style-type: none"> • Qld Land Titles • NSW Land Titles • Vic. Land Titles • WA Land Titles • ACT Land Titles
Transport and Police Searches	<ul style="list-style-type: none"> • Qld Vehicle Registrations** • Qld Traffic Incident Reports** • Qld Crime Reports**
Legal Lodgments and Searches	<ul style="list-style-type: none"> • Victorian Magistrates Courts** • Victorian Magistrates Courts Default • Complaints • Order Requests • Warrants to Seize Property • Summons for Oral Examination
Victorian Liquor Licences	<ul style="list-style-type: none"> • Copy of Licence • Premises and Licensee Name • Applications Lodged and Granted • Licence Location and Type • Inquiry

Source: CITEC CONFIRM

Note: ** denotes restricted database

otherwise accessed by making an over-the-counter request to the relevant agency or department. With the unrestricted databases now accessible via the Internet, the service is available

to anyone in the world. To use the service, clients must register and receive an account code and password. All usage is logged to their account code, thus providing an audit trail. Information

can be accessed via the Internet or by dialling into CITEC's own communications network.

The databases of interest to this Inquiry are the three restricted databases that belong to the QPS and Queensland Transport:

- Traffic Incident Recording System (TIRS), owned by the QPS
- Crime Reporting Information System for Police (CRISP), owned by the QPS
- Queensland Motor Vehicle Registration (QMVR) database, owned by Queensland Transport.

To obtain access to these restricted databases the user must complete an additional application form, stating the reason for requiring access. The application is forwarded to the owner-agency of the database, which either approves or denies access. The following sections describe the information available on each database and outlines the application process.

TIRS and CRISP, owned by the QPS

Through TIRS, authorised users have access to details of traffic incidents, such as:

- date of the incident
- contributing circumstances
- location of the incident
- vehicle information, type, registration, make and number
- witnesses' versions
- ownership details of vehicles involved
- blood-alcohol levels
- victims and injuries.

Through CRISP, authorised users have access to details of property crimes, such as:

- summary of the crime details (e.g. crime number, address of offence etc.)
- complainant details
- informant/witness details
- property details
- modus operandi
- other crime classes (i.e. additional crimes committed)
- recovery details of property.

Appendix Q provides more detail on the types of information, reports and documents that are available to authorised users of TIRS and CRISP.

The categories of users that are eligible to apply for access to TIRS are insurance companies, legal firms, loss assessors and mercantile agents. Access to CRISP is limited to insurance companies and loss assessors.

An estimated 385 clients have been granted access to TIRS, and the majority of these are legal firms. For CRISP, 33 clients have been granted access, the majority being insurance companies. A breakdown of access by type of business is shown in table 7.3 on page 83.

To be granted access to either system, the business and the individuals in the business requiring access must complete an application form and a confidentiality agreement. All forms remind the applicant that unauthorised access to and/or release of information will render the user liable to prosecution. The confidentiality form also includes an agreement that checks will only be conducted as authorised in the course of work duties.

A business must show that it meets the criteria for TIRS and CRISP access (e.g. establish its bona fides as a loss assessor). The QPS also considers the character, honesty and integrity of individual users before granting access. This process includes having regard to any previous criminal convictions and other matters of relevance to the QPS. Access is not granted where a business or individual does not meet the criteria, or is considered by QPS to be an unacceptable risk, or has demonstrated an inability to act responsibly. Individual applications must be accompanied by a signed confidentiality agreement (figure 7.5).


Once authorised, the client signs an agreement with the State of Queensland (through CITEC) on conditions of use of TIRS and/or CRISP. Access to TIRS and CRISP is through the private dial-up to the CITEC network (as opposed to the Internet). Users must first enter a Traffic Incident Number (TIN) or CRISP number. They are then presented with summary details indicating the address of the incident or crime and the type (e.g. burglary, stolen vehicle). They confirm they have the correct claim by pressing 'Enter', which brings them to the 'Reason for Transaction' screen (appendix R). Either the 'Claim No.' field (see appendix R) or the 'Reason' field is mandatory for entry, but the response is not validated. The other fields are not mandatory. When CITEC is making an inquiry on behalf of a client who does not have direct access, they enter 'accessing crime report' against reason and under 'representing'

Table 7.3 — Access to TIRS and CRISP by category of business

CATEGORY OF BUSINESS	NUMBER WITH ACCESS TO CRISP	NUMBER WITH ACCESS TO TIRS
Insurance companies	20	32
Legal firms	0	324
Loss assessors	13	9
Mercantile agents	0	8
Other	0	12
TOTAL AUTHORISED USERS	33	385

Source: PIC and CITEC CONFIRM (July 2000)

Figure 7.5 — Confidentiality agreement for application for access to TIRS or CRISP



CITEC CONFIRM
 Quality Form: PASFM020
 Application for Individual Access to the Crime Reporting Information System for Police (CRISP)

Confidentiality Agreement
(APPLICANT TO COMPLETE -Mandatory)

I, _____
(Full Name)

Being attached to _____
(Organisation Name)

hereby acknowledge that I have been given access to certain areas of the Queensland Police Service computer system.

I agree to make only such checks on that computer system as may be authorised in the course of my duty at (Organisation Name) _____ and to treat all information which I obtain from that computer system as confidential.

I will not make any unauthorised checks on the computer system, nor will I release or otherwise deal with any information from that computer system in any manner which has not been approved by my superiors.

I acknowledge that if I breach this agreement I may be liable to have action taken against me under The Commonwealth Crimes Act 1914 or any other Statute as applicable.

Dated at _____

This _____ day of _____ 1999

Signature
(Applicant)

Witness to Signature
(Client CRISP Information Security Office or other Authorised Person)

(CLIENT SERVICES TO COMPLETE)

User ID: _____ Password: _____

Advised By: _____ Date: _____

Work Instruction Reference: PASWI010
 Commercial-in-Confidence
 Copyright
 Issue No. 06 - Page last updated 23/11/99

Note: The confidentiality agreements for TIRS and CRISP are identical.

they enter the name of the client (this can be a company name).

If users wish to obtain one of the reports or documents (as shown in appendix Q), they can be ordered on-line for counter pick-up or postal delivery. The prices charged for documents and reports are shown in appendix S. For access to each database, users are required to maintain a Movement Log to record distribution of reports, or copies thereof. For example, the log for TIRS must include the following details:

- a) the TIN
- b) the destination of the Traffic Incident Report and copies thereof
- c) the claim number or file number
- d) the reason for distribution
- e) the name of the organisation or individual they are representing in relation to the matter being dealt with.

The TIRS and CRISP systems accessed through CITEC will generate security activity and audit logs that show the queried data that are displayed to the user. QPS has the right to audit these logs. If any concern is raised, the user can be asked to provide documentation to justify access, and to confirm the reason for access that the user has submitted. The Movement Log may also be audited to establish that the distribution of reports and copies has been for agreed purposes. If a business or user has breached the agreement, access can be terminated.

Two audits have been conducted, one by the ESC and one jointly by ESC and ISS. Proactive audits have not been undertaken to date. These are scheduled to be carried out by the ISS when resources allow.

Queensland Motor Vehicle Registration (QMVR) database, owned by Queensland Transport

This database contains current and historical details about motor vehicles, vessels, caravans and trailers. A number of third-party insurers and government agencies can conduct searches of this database by name through CITEC CONFIRM.

Driver's licence records are not available through CITEC CONFIRM, but clients do have access to the registration database through CITEC CONFIRM.

Other authorised users of CITEC CONFIRM can only conduct a search by vehicle registration number; a search cannot be conducted by a

person's name. The information that the authorised user can access is:

- the name in which the vehicle or vessel is registered
- the address of the registered operator
- the engine number of the vehicle or vessel
- the identity of the compulsory third-party insurer.

The policies relating to the release of information by Queensland Transport have recently changed. The National Road Transport Commission has sought to develop a national standard for the management, use and release of registration and licensing information. It is critical to have a national standard because the National Exchange of Vehicle and Driver Information System (NEVDIS) allows access to information held by other States and Territories. A national standard ensures consistency across states and territories on the release of registration and licensing information.

Queensland Transport recently reviewed the legislation and policies on the release of information and in November 1999 announced new policy guidelines. The new guidelines, for which implementation commenced on 1 January 2000, state:

A person is entitled to apply to search the registration database where legal action or proposed legal action involves the motor vehicle for matters:-

- about an incident on a road or elsewhere,
- about bankruptcy proceedings,
- about fraudulent activities, or
- before the Family Court of Australia. (Queensland Transport Policy 2000)

Also at that time, Queensland Transport wrote to all CITEC CONFIRM clients who had access to the Queensland Transport database announcing the change and advising their clients to re-apply for access to the Register of Vehicles by 1 January 2000. Under the new application process, applicants must indicate the type of business conducted and provide statutory evidence that supports their entitlement to the motor-vehicle registration database. One of the following reasons for access must be ticked off, and proof given of the need for access:

- accident (motor-vehicle/ship incident)
- legal (bankruptcy, family court, fraud)

- local authority (regulated parking)
- government
- statutory authority
- court
- other (details must be provided).

Since 1 January 2000, an estimated 171 CITEC CONFIRM clients have had access rights to the motor vehicle registration database revoked. In addition, 250 CITEC CONFIRM clients failed to reapply for entitlement to access the register of vehicles and consequently had their access withdrawn.

The basis for revoking access for many of these clients was that their eligibility was not demonstrated in their entitlement application, having regard to ss. 67 and 68²² of the **Transport Operations (Road Use Management Vehicle Registration) Regulation 1999**. These sections concern the provision, to 'eligible persons', of an extract from the register of information about a vehicle.

The majority of these clients were private investigators, debt collectors, loss adjusters and finance companies. There are an estimated 793 clients who currently have access to the database through CITEC CONFIRM. These clients include legal practitioners, insurance companies, local-government agencies, government departments and statutory authorities. The cost for a check on a current registration is \$10.00 (see appendix S for costs of other searches).

Once granted access to the database via CITEC CONFIRM, users are not required to complete a reason for transaction for each search. However, as agreed to in the access contract with Queensland Transport, users must maintain adequate records to justify access to the specific record within the database. By keeping these records, Queensland Transport can later undertake a 'reason for access' audit on all CITEC CONFIRM clients who have had access to the registration database. The current program of random audit will be implemented after 12 months of reviewing clients' entitlements.

The Institute of Mercantile Agents told the CJC that Queensland Transport has advised that, after 10 March 2000, it will no longer provide previously available information to licensed commercial agents. Queensland Transport has informed the CJC that the reason for this action is that mercantile agents and licensed commercial agents are not eligible under s 67 of the **Transport Operations (Road Use Management Vehicle Registration) Regulation 1999** to have direct on-line access.

They are, however, able to submit individual search applications to Queensland Transport's customer-service centres with supporting documentation if their search is within s 67 of the **Transport Operations (Road Use Management Vehicle Registration) Regulation 1999**.

Users can conduct a name search through Queensland Transport. Applicants must provide the full name and last known address of the person or organisation in question, and the information sought must be within the Release of Information guidelines as defined in the **Transport Operations (Road Use Management Vehicle Registration) Regulation 1999**.

The Institute of Mercantile Agents was also critical of the search facility because a search on a single name, say 'Smith', might result in 50 responses, for which the applicant would be charged. In response, Queensland Transport argued that this should not occur because of the requirement for applicants to provide the full name and last known address of the person who is the subject of the search.

The PIC

Under s. 10.2 of the PSAA, the Commissioner of Police can authorise the disclosure of confidential police information:

10.2 (1) The commissioner may, in writing, authorise disclosure of information that is in the possession of the Police Service.

(1A) Authorisation under subsection (1) must accord with any regulations made in relation to disclosure of such information, and any such authorisation is to be taken as authorising disclosure in accordance with any such regulations.

(1B) Also, subject to any regulation made under subsection (1A), the commissioner may impose conditions on the disclosure of information under this section.

(1C) A person to whom the information is disclosed must not contravene a condition imposed under subsection (1B).

Maximum penalty — 40 penalty units.

(2) Neither the Crown nor any person incurs any liability in law on account of a disclosure of information made under and in accordance with the commissioner's authorisation.

Section 10.2 is restricted in its operation and does not constitute an authority to disclose information otherwise prohibited by legislation. For instance, provisions of the **Criminal Law (Rehabilitation of Offenders) Act 1986** apply.

The Manager of the PIC has been delegated the authority under s 10.2 to disclose information held by the police. The functional areas of PIC are Information Policy, Crime Management, Offender Management and the Information Service Centre, which includes the Help Desk, the Information Service Unit, the Information Support Unit and the Warrant Bureau.

The PIC provides members of the public with documents that are produced as part of the prosecution process or from criminal-history information. Members of the public can apply at their local police station for these documents. The PIC also has an overseeing role in relation to the release of crime reports through CITEC CONFIRM.

The documents available to members of the public are a Court Brief, criminal history, record of charges, and Police Certificate. Members of the public can obtain a copy of a Court Brief (QP 9)²³ from the PIC if it contains information about them or relates to the exercise of a right that may be available to them (e.g. criminal-injury compensation). A Court Brief is only provided where the court proceedings have been finalised and the appeal period, if any, has expired. Personal information relating to a person other than the applicant is deleted from the document (e.g. complainant details are erased before release to the offender).

The criminal-history record of a person includes the convictions that the person has incurred in Queensland and the disclosable cautions and disclosable community-conference agreements (see ss 18N and 18O of the *Juvenile Justice Act 1992*). This document is usually sought by individuals for court-related purposes. It is only released to the person concerned, or to the person's legal representative, at the express wish of the person.

The 'record of charges' is a record of all charges that have been preferred against a person by QPS officers, regardless of the court outcome, and also includes all cautions and community-conference agreements administered or made under the *Juvenile Justice Act 1992*. It is only released to the person concerned, or to the person's legal representative, at the express wish of the person.

A National Police Certificate contains a certification that the person to whom the document relates either has no disclosable convictions or has a disclosable conviction that is detailed in the Certificate. If there are disclosable convictions recorded in any State or Territory, including Queensland, they will appear in the Police Certificate. A disclosable conviction is a

conviction that is recorded and the disclosure of which to any person does not breach the *Criminal Law (Rehabilitation of Offenders) Act 1986*, the *Penalties and Sentences Act 1992*, the *Juvenile Justice Act 1992*, or the *Crimes Act 1914* (Cwlth). For this reason, they are usually sought for employment or visa purposes and only released to the person concerned or, in the case of a visa application, to the nominated consulate.

The charges for the provision of the above-mentioned documents are shown in table 7.4 on page 87.

Criminal-history information is confidential and is not usually disclosed to interested third parties unless to do so is in compliance with a statutory requirement or the third party is a law-enforcement agency. This information is not provided to inquiring third parties such as legal firms, private inquiry agents, commercial agents and insurance companies. The PIC may, in certain circumstances, advise a third party that the person who is the subject of the inquiry has no disclosable criminal history, but this is only with the knowledge and written consent of the person concerned. Where the person has a conviction that is disclosable, that person can obtain a Police Certificate from the PIC that details the conviction. It is then a matter for the person concerned to consider the disclosure of the conviction to any other person or organisation.

Other confidential information is protected and, in the absence of a legislative requirement for the QPS to disclose the information, it will only be released to a third party when warranted in the circumstances (e.g. where disclosure is necessary to protect the health and safety of a person). Such disclosures are made only when they are consistent with the functions of the QPS. It is also necessary for an inquirer to demonstrate a legitimate and sufficient interest in obtaining the information.

The disclosure of confidential information to third parties for purposes not associated with, or contributing to, the primary role and objectives of the QPS is made only in exceptional circumstances. The location of parties to civil proceedings and civil debtors is normally not a function of the QPS. Requests for information about the whereabouts of such people, if received from private-sector organisations such as lawyers, private inquiry agents, commercial agents, or similar, would be viewed accordingly. As a general rule, requests from private organisations are not granted.

Table 7.4 — Fees for documents provided by the Police Information Centre

DOCUMENT	FEE CHARGED
Court Brief (QP 9)	\$15.00
Copy of own Queensland criminal history	\$33.30
Copy of own Queensland record of charges	\$33.30
National Police Certificate (name check only)	\$34.00
National Police Certificate name check and fingerprint search)	\$120.00

(Source: PIC July 2000)

Requests for information on traffic incidents and crime reports relating to property offences are generally directed to CITEC CONFIRM. The OPM policy on requests for Queensland vehicle-registration and driver's licence details is for members of the QPS to refer such requests to Queensland Transport.

Queensland Transport

Members of the public and representatives of organisations can approach Queensland Transport directly for a one-off request for information in accordance with the new information-release policies outlined on page 84. They can walk into a Customer Service Centre and complete a 'Search of Vehicle/Recreational Ship Registration Records Request'.

The applicant must provide documentation that supports the claim that the search, which must be for matters involving a motor vehicle, is necessary and legitimate. Documents that are acceptable are motor-vehicle/police incident reports, repair quotes and statutory declarations, insurance company letters, and court/legal documents or statutory declarations about a legal process or proposed legal process involving the motor vehicle. Proof of identification is also necessary. The following information can be provided:

- registered operator name
- address
- registration number
- engine number
- compulsory third party insurer
- other (specify the information required).

The search is performed by a Queensland Transport employee on behalf of the applicant, and the typical charge is \$10.15 for an extract of a registered operator's name and address, and \$16.25 for an archival search. The application

forms are stored with the operator's files and sent to a document-retention area.

WHY ARE PRIVATE INVESTIGATORS BEING EMPLOYED TO OBTAIN ILLICIT INFORMATION?

Given the lawful avenues by which information can be obtained, the question that must be answered is why the cleaner at Nerang Station (N1) and the private investigator (N2) chose to obtain information by unlawful means.

At the conclusion of its Inquiry, the ICAC (1992a) found three reasons for such conduct:

- There had not, in the past, been any consistent policy to determine what information should, and what information should not, be available to the public.
- Obtaining publicly available information has frequently been subject to such delays that a parallel illicit trade has developed, with greater speed its prime selling point.
- Information that has been held as confidential has generally not been well protected and rudimentary precautions have not been taken with the systems that have been in place.

Once again, it should be noted that, unlike the ICAC's investigation, the CJC's investigation did not extend beyond the police service. The CJC is not, therefore, in a position to comment on the whole-of-government approach to policies relating to information management. However, in respect of the latter two points, there are parallels in Queensland. The issue of adequate protection is covered in chapter 6 ('Improving Information Security in the QPS') and will not be further discussed here. The issue of availability and speed is the topic of the remainder of this section.

The cleaner at the Nerang Police Station, N1, spoke of the ease with which he could obtain information from police stationed there. When

asked by Counsel Assisting why he did not obtain the information through alternative sources, he replied 'Probably didn't think about it, and possibly the convenience the way I was getting things and the speed' (CJC unpub., p. 238). He later agreed with Counsel Assisting that he continued to seek information in this way because it was 'reliable, speedy and cheap' (p. 238).

But this does not fully explain the illicit trade in information. CITEC CONFIRM, in particular, provides a very efficient means of obtaining certain information. Furthermore, cost comparison between the charges of the private investigator and those of CITEC CONFIRM show minimal differences for obtaining the same information.

The answer really lies in the fact that the information that is lawfully available is not available for every reason for which an end-user may require it. When one examines table 7.1 (p. 78), none of the stated reasons for requiring the information would have entitled the end-user to access any of the information held by the Department of Transport or the QPS. However, if the reasons are genuine, few would argue that, in most of the examples, the end-user had a legitimate reason to obtain the information.

During submissions to the CJC, the Queensland Law Society provided examples of situations where the legal profession required access to confidential information. The Society submitted that, while some information can be obtained through legitimate means, there are problems with motor-vehicle searches because of the limited purposes for which information can be obtained (see page 84). The Society gave examples of situations where information is not available:

- Criminal-compensation cases — the **Criminal Offence Victims Act 1995** (s. 28(1)) provides that, before an application to a court for a compensation or repayment order against a convicted person is decided, the convicted person must be notified of the application. The Society was of the view that, whereas motor-vehicle and driver's licence searches would assist in locating the convicted person so that he or she could be notified of the application, the facility is not available for that purpose.
- Locating offenders for the purpose of service and obtaining details of assets. Details of the addresses of offenders are not allowed to be provided by Corrective Services²⁴ or Queensland Transport. Similarly, the QPS does not, as a general rule, release

information to third parties for this purpose.

- Litigation — In civil cases where a witness's credibility is at issue, the fact that the witness has a criminal record will usually be significant. In criminal trials the defence is entitled to copies of the criminal histories of the defendant, the complainant and other witnesses. However, this is not the case in civil litigation, which may concern disagreements over important issues such as the custody of children, disbursement of property, liability for injury or loss, or defamation. There are many other examples. The Law Society favours a rule that the parties may apply to the relevant court for an order directing the QPS to release a person's criminal history for the purpose of preparing for, and conducting, litigation. In the Society's view, the court is better placed to give due consideration to the merits of the application.
- Locating debtors for the purpose of serving legal process and executing judgments — Many 'professional' debt evaders ensure that their details cannot be found on publicly available databases (e.g. electoral rolls, lands and property titles, etc.). Queensland Transport will not provide an address from the motor-vehicle registration database if the documents do not relate to a motor-vehicle incident, bankruptcy proceedings, fraudulent activities or matters before the Family Courts. Similarly, the QPS does not generally release information to third parties under these circumstances.
- Conducting investigations in the preparation for litigation — a simple example will suffice here. When preparing a case for their clients, solicitors need to locate a number of possible witnesses. Publicly available databases are of no assistance. Under the present regime, the solicitor cannot access the Department of Transport or QPS database for information as to the whereabouts of the witnesses.

The Institute of Mercantile Agents also provided a written submission (2000):

I would like to submit on behalf of our members in respect of motor vehicle theft or insurance fraud that police resources are stretched when investigat[ing] these matters. We believe only token or no investigations regularly result. Allowing access to current and historical vehicle registration records would assist legitimate investigations.

The Institute also submitted examples of other situations where it considers that information

should be made available but where current provisions do not allow lawful access:

- companies engaged to provide security for property and individuals who need to obtain details of suspicious vehicles
- companies employed to locate missing persons where there are genuine fears for safety
- companies employed by a parent/guardian to locate a child who is addicted to drugs and is 'in danger of falling into a life of crime, death or ruined health'
- criminal histories for whatever purposes, given that, at the time of the court cases, the details would have been published in the paper and documented in court records, which are publicly available.

The question of accessing criminal histories has been the subject of considerable debate, not only as a result of this Inquiry but also because of the recent development of a publicly accessible website that lists criminal histories.

It is true that criminal histories are generally published in the court at the time of sentencing. Criminal courts in this country operate in an open and transparent manner. When a person is convicted of a criminal offence and sentenced, the proceedings are open to the public. It is also permissible to report the proceedings in the electronic and print media, and in only a few types of cases will certain details be suppressed. In general, the matter may be reported as often as it is newsworthy or of interest to the public. In some cases a matter may be reported again years after the event — e.g. when a notorious prisoner is released.

However, although criminal proceedings are held in public, it is another thing entirely for any member of the public to be able to access, on request, a comprehensive and accurate criminal record that can be used at whim. The damage to the convicted person could be considerable.

Perhaps the most significant issue here is the need to rehabilitate offenders. While this is a complex issue, a key prerequisite for successful rehabilitation is the opportunity for the offender to be a dignified and productive member of the community. This principle is recognised by statute.

The **Criminal Law (Rehabilitation of Offenders) Act 1986** sets out the legislative requirements regarding disclosure of criminal histories. This Act stipulates that the rehabilitation period for a conviction for an indictable offence is ten years;

for all other offences the period is five years.²⁵ After the expiration of the rehabilitation period, and providing that there has not been a revival of the conviction, it is lawful for offenders to claim, upon oath or otherwise, that they have not suffered a conviction. (The only exceptions can be found in ss. 4 and 9 of this Act.)

The concept of rehabilitation is hardly consistent with the notion that a person's criminal record should be freely available for publication at any time. It could be used in a most malicious way: to ostracise the person, or to unfairly deny them a job.

The other significant categories of information that were sought were driver's licence and vehicle-registration details. By searching databases holding this information, the most up-to-date information on the whereabouts of the licence holder and/or registered owner can be obtained. Armed with this information, those requesting it could attempt to locate the person who was the subject of the search.

Again, there are many understandable reasons why a person needs to be found (as noted above). Unfortunately, there are also examples of people wanting to locate someone for sinister reasons. The CJC heard evidence of some of these; this evidence is summarised in chapter 3 ('The Investigation'). It follows that unrestricted access to these databases is unacceptable.

Many of the reasons for accessing confidential information that were given by those who appeared before the CJC are persuasive, but there are also persuasive arguments against such disclosure. Fundamentally, the right to privacy of information must be considered when developing any government policy on the release of information.

Furthermore, the CJC is concerned that there is presently insufficient education and training required before a commercial agent's and private investigator's licence is granted. In the CJC's view, the absence of such a requirement has contributed to malpractice and unlawful conduct in the industry. The other concern of the CJC is the lack of controls and regulations to uphold professionalism and integrity with both industries. Until this lack is remedied, the CJC is most reluctant to extend the capacity of commercial agents and private investigators to access confidential information held in government databases. This issue is discussed at greater length in the next chapter.

In the CJC's opinion, the Government should review the restrictions that currently apply to accessing criminal histories and driver's licence

and vehicle-registration particulars to determine whether any of those restrictions can be varied or waived in some cases.

RECOMMENDATION 7.1 — ACCESS TO CRIMINAL-HISTORY, DRIVER’S-LICENCE AND VEHICLE-REGISTRATION RECORDS

That the Government review the restrictions that currently apply to accessing criminal histories and driver’s licence and vehicle-registration particulars to determine whether any of those restrictions can be varied or waived in certain cases.

CONCLUSION

The observations made during this Inquiry were not surprisingly different from those made during the ICAC Inquiry (1992). In the majority of instances this type of misconduct occurred in response to an information request from an unauthorised third party. It became apparent that private investigators and commercial agents often serve as the information brokers who obtain information on behalf of clients, the majority of whom are private-sector businesses.

Within Queensland, confidential information of the type of interest to this Inquiry can be lawfully released by CITEC CONFIRM, the QPS PIC and Queensland Transport. Each organisation has rules and guidelines on who should be granted access to restricted databases. CITEC CONFIRM provides information efficiently and at a cost comparable with that seen in the illicit information market. It became apparent that illicit means were used because the individuals and organisations seeking information will not be granted access to restricted information under current government policy.

Although some reasons for seeking information had a questionable justification, many reasons appeared legitimate (e.g. locating individuals in order to serve legal process and execute judgments). As a result, the CJC has recommended that the Government review the restrictions that currently apply to accessing criminal histories and driver’s licence and vehicle-registration particulars to determine whether any of those restrictions can be varied or waived in some cases.

INDUSTRY REGULATION IN QUEENSLAND

During the Inquiry, statements and submissions were heard from the IMA (Institute of Mercantile Agents) for increased access to information, particularly current and historical vehicle-registration records. As noted in the previous chapter, this access has recently become more restrictive with recent changes to Queensland Transport policies. It would be expected that private investigators would similarly argue for increased access to information, as was found in the ICAC Inquiry.

The CJC expressed the view that there are presently insufficient education and training requirements and inadequate government regulation of these industries to recommend that these occupations be granted access to confidential government information. This chapter begins by discussing the comments and observations of the ICAC Inquiry into the release of confidential government information (1992a). This is followed by some examples of the evidence heard during the CJC public hearing that caused concern for the CJC and resulted in its taking a closer look at the systems of regulation.

The purpose of the remainder of this chapter is to provide an overview of the current legislative regime and industry practices to identify improvements that will help to raise the level of professionalism and integrity within each industry. Commercial agents and private investigators are discussed separately because they are subject to different regulation. For each industry, the following issues are examined:

- legal definition of the occupation
- applying for a licence
- licence renewal, suspension and disqualification
- training, education and professional development
- non-government regulation.

In the remaining sections, comments are made on industry regulation and, where necessary, recommendations are made for improvement.

THE CONCERN ABOUT THE INDUSTRIES

It was observed during the ICAC Inquiry (1992a) that almost all of the information uncovered during the ICAC investigation was found to have been released by government department and agency employees into the hands of private investigators (this term, as used in the ICAC report, refers collectively to private investigators, commercial agents and sub-agents and those who were not licensed but who carried on a similar business). It was further commented that 'disclosures made to the Commission establish a need to look closely at the private investigation industry' (ICAC 1992a, p. 117).

The ICAC concluded that, if being a licensed private investigator or commercial agent were to be the qualification for obtaining confidential information, there would have to be much stricter licensing requirements because of the number of licensed persons who, in the course of the investigation, admitted:

- (a) lying on oath;
- (b) deliberately deceiving government departments and agencies in order to obtain information;
- (c) corruptly paying public officials to release information in violation of their duty, and
- (d) ignoring criminal sanctions contained in both State and Commonwealth legislation. (ICAC 1992a, p. 121)

The report makes many recommendations to improve industry regulation, including requirements for qualifications, the establishment of a code of conduct and regular and spot checks on accounts and records of licensees. The full list of ICAC recommendations and the comments on them can be found in appendix U.

Although the CJC Inquiry was not as extensive as the ICAC Inquiry, evidence was heard that raised concern about industry regulation for private investigators and commercial agents in Queensland. One private investigator commented

on the usefulness of his private investigator's licence:

Can I say this, that I started my business as an investigator in 1984, that's 17 years ago. I was given a licence to practise as a private investigator, I didn't have to undergo any test to do it. In the years since I've paid the government X amount of dollars per year to retain that licence. Never once in 17 years have I had that licence off my wall or out of my pocket for the simple reason that nobody cares, nobody wants to see it. (CJC unpub., p. 445)

It was also alarming that this private investigator (N2) knew, and was not deterred by, the fact that the information he was being provided with came from police sources.

Counsel Assisting: And how did you get to know [where the cleaner got the information from]?

N2: Because he — he asked me for information from my own databank and he said that 'a policeman mate of mine' or a copper mate of his, to use the vernacular, was interested in a particular person and 'Can I have a look at' — well, could he have a look at the file and take copies of it, and he said, 'I can get you a couple of checks done,' so I knew that he was doing that directly through the police. (p. 426)

N2 recalled there was at least one other private investigator he dealt with who had 'police contacts':

Counsel Assisting: The request for information [to locate a person] written by you on 15 October. Would you look at [slide] 59? The day before [another private investigator] signs off the information a police officer called [name] has done a search from Beenleigh on [name of person to be located]?

N2: Right.

Counsel Assisting: It was well and truly apparent to you that he could supply police information?

N2: Yeah, I must say I'd forgotten all about that. Yep. (p. 442)

Similarly, the cleaner at the Nerang Police Station (N1), who supplied information to N2, and was effectively operating as an unlicensed private investigator/commercial agent, admitted to stealing print-outs that contained confidential information:

Counsel Assisting: ... it's been suggested by some witnesses that you may have adopted this practice: requested a police officer for

information, observed a print-out being created of the information requested and biding your time to a period later in the day and on your rounds of cleaning up the office fishing out the police print-out keeping it and destroying all other surplus material according to your task as a cleaner; what do you say to that suggestion as a possibility for your behaviour?

N1: It's a possibility, yes.

Counsel Assisting: So do you agree and you may wish to make a claim on this but do you agree that without the knowledge of some officers you removed police print-outs?

[Witness makes claim but is instructed to answer the question.]

N1: Yes. (CJC unpub., p. 236)

He also indicated that he was aware that his actions were wrong:

Counsel Assisting: You have already acknowledged that you knew what you were doing was unlawful?

N1: Yes.

Counsel Assisting: You were asking sworn police officers to therefore act unlawfully or wrongly?

N1: Yes.

Chairman: And the only risk you ran at Nerang was a risk of a knock-back?

N1: Yes. (CJC unpub., p. 243)

These comments, along with the benefit of the experience of the ICAC, prompted the CJC to take a closer look at industry regulation for commercial agents and private investigators. The effectiveness of industry regulation in these areas is relevant in considering how to prevent the improper release of information held on government databases. For example, the CJC considered industry regulation to be highly relevant to whether it could recommend increased access to government information by commercial agents and private investigators.

COMMERCIAL AGENTS

Governing legislation

At the time of writing, commercial agents are regulated through the *Auctioneers and Agents Act 1971*. However, on 26 July 2000, the Minister for Fair Trading released for public comment the draft of the *Property Agents and Motor Dealers Bill 2000*. The objectives of the proposed legislation are 'to modernise the law to create greater flexibility in dealing with the evolving business environment and to introduce new

consumer protection measures to overcome deficiencies identified in the existing Act'.²⁶

The Bill was introduced into Parliament on 7 September 2000 and is currently awaiting debate.²⁷ For the purposes of this report, the CJC has considered the proposed regulatory system provided by the draft Bill rather than the Auctioneers and Agents Act. Several issues of concern to the CJC have already been addressed within the draft Bill, in particular the eligibility of persons to be licensed, the proposed disciplinary regime and, of course, ongoing education. The effectiveness of these proposals remains to be seen.

The Office of Fair Trading, which is within the Department of Equity and Fair Trading, is responsible for the administration of the Auctioneers and Agents Act and maintaining the register of licensed businesses/operators.

Legal definition of 'commercial agent'

In the draft Bill, a commercial agent is defined by the duties or activities authorised by the licence.

326.(1) A commercial agent's licence authorises the holder of the licence ('commercial agent') to perform the following activities as an agent for others for reward —

- (a) to find, or repossess, for a person any goods or chattels that the person is entitled to repossess under an agreement;
 - (b) to collect, or request payment of, debts;
 - (c) to serve any writ, claim, application, summons or other process.
- (2) A commercial agent may perform the activities in the carrying on of a business, either alone or with others, or as an employee of someone else.

Application and eligibility for a licence

To operate as a commercial agent a person must obtain a property agent's and motor dealer's licence (commercial agent).²⁸ Section 26 provides that a person is not a suitable person to hold a licence (which includes a commercial agent's licence) if the person is —

- (a) an undischarged bankrupt; or
- (b) a person who has been convicted, in Queensland or elsewhere, within the preceding 5 years of a serious offence; or
- (c) currently disqualified from holding a licence; or
- (d) a person the chief executive decides under section 28 is not a suitable person to hold a licence.

Similarly, under s. 27, a corporation is not a suitable person to hold a licence if an executive officer of the corporation is —

- (a) an undischarged bankrupt; or
- (b) a person who has been convicted, in Queensland or elsewhere, within the preceding 5 years of a serious offence; or
- (c) a person the chief executive decides under section 28 is not a suitable person to hold a licence.

Section 28(1) provides that the chief executive must, when deciding whether someone is a suitable person to hold a licence, consider the following things:

- (a) the character of the person;
- (b) the character of the person's business associates;
- (c) whether the person held a licence under this Act, the repealed Act or a corresponding law that was suspended or cancelled;
- (d) whether an amount has been paid from the fund because the person did, or omitted to do, something that gave rise to the claim against the fund;
- (e) whether the person has been disqualified under this Act, the repealed Act or a corresponding law from being a licensee or an executive officer of a corporation;
- (f) for an individual —
 - (i) the person's criminal history; and
 - (ii) whether the person has compounded with creditors or otherwise taken, or applied to take, advantage of any law about bankruptcy; and
 - (iii) whether the person has been convicted of an offence against this Act or the repealed Act or a corresponding law;
 - (iv) whether the person is capable of satisfactorily performing the activities of a licensee;
 - (v) whether the person's name appears in the register of disqualified company directors and other officers under the Corporations Law;
- (g) for a corporation—
 - (i) whether the corporation has been placed in a receivership or liquidation; and
 - (ii) whether an executive officer of the

corporation has compounded with creditors or otherwise taken, or applied to take, advantage of any law about bankruptcy; and

(iii) whether an executive officer of the corporation has been convicted of an offence against this Act or the repealed Act; and

(iv) whether each executive officer of the corporation is a suitable person to hold a licence;

(h) another thing the chief executive may consider under this Act or a regulation.

The chief executive may make investigations about the applicant or licensee (including a corporation) and a business associate of the applicant or the licensee to help him/her decide whether such an applicant or licensee is a suitable person to hold a licence (s. 31(1)). The chief executive may ask the Commissioner of the Police Service for a written report about the criminal history of any of the persons (s. 31(2)).

To be eligible to obtain a commercial agent's licence, the individual must be at least 18 years old and have the educational or other qualifications for a commercial agent's licence that may be prescribed under a regulation (s. 44(1)(b)). At the time of writing, no regulations were publicly available, so the CJC is not aware of the standards or course content envisaged by the Department.

A corporation can only be granted a commercial agent's licence if at least one of its directors is licensed as a commercial agent (s. 44(3)). The chief executive may place conditions on a licence that limit or prohibit the performance of an activity authorised under the Bill or require the licensee to hold insurance of a kind and in an amount prescribed under a regulation (s. 50)).

Licence renewal

The term for a licence can be one or three years. Before the licence is due to expire, the licensee must apply for its renewal (s. 54(1)). The application must be accompanied by, among other things, an audit report for all trust accounts kept by the licensee or a statutory declaration that the licensee did not operate a trust account during the audit period (s. 54(3)). Individuals applying for renewal must also submit two recent, certified colour photographs of themselves (s. 54(2)(d)(iv)). In granting renewal, the chief executive officer must be satisfied that the licensee is a suitable person (s. 55(2)(a)), has actively carried out the activities authorised under the licence (s. 55(2)(c)) and meets the eligibility

requirements for the licence (s. 55(2)(d)).

The chief executive may immediately suspend a licence if an irregularity or deficiency exists in a licensee's trust account or if a receiver is appointed (ss. 71(1) and (2)). The licence must be returned to the chief executive within 14 days of the licensee's being notified of the suspension (s. 71(5)). Similarly, a licence can be immediately cancelled if the licensee is convicted of a serious offence, if the licensee is an undischarged bankrupt or — if the licensee is a corporation (s. 72(1)) — the licensee has gone into liquidation.

Employees

Chapter 3 ('Employee Registration') of the draft Bill provides for the registration of certain categories of employees, including commercial sub-agents. An application for registration is similar to that for obtaining a licence in that the individual must be suitable to hold registration. The suitability criteria for registration are the same as those applied to licence applicants. Once application for registration is successful, the employee receives a registration certificate that is valid for a one- or three-year term. The certificate allows the employee to perform any activity that may be performed by a commercial agent by whom the holder is employed unless the chief executive imposes conditions on the certificate. In addition, the certificate is not transferable. The provisions for immediate suspension or cancellation of registration certificates are the same as those for licence suspension and cancellation.

Section 327 of the draft Bill makes it the responsibility of the principal licensee or licensee in charge of a commercial agent's business to ensure that each commercial sub-agent is properly supervised, acts only within the scope of his/her authority and complies with the Act (draft Bill). Failure to do so can result in disciplinary action being taken.

How the agent or business operates

Section 337 provides for the enactment of a code of conduct in respect of commercial-agency practice:

337. A regulation may prescribe a code of conduct about commercial agency practice that may include the following —

- (a) setting conduct standards for commercial agents and commercial sub-agents;
- (b) establishing principles for fair trading;
- (c) providing for a system of complaint resolution.

Other sections provide that:

- an individual in charge of a commercial agent that is a corporation must be a registered commercial agent (s. 330(2)(a))
- a commercial agent who is asked to provide services specified in the Act must be appointed, in writing, by the client (s. 331(1))
- commission and recoverable costs are to be calculated in a prescribed manner
- trust accounts and funds are to be monitored, audited and administered lawfully
- freezes can be placed on accounts, and receivers and special investigators can be appointed.

The draft Bill also allows for the establishment of a claim fund.

Chapter 15 ('Enforcement') of the draft Bill includes provisions to appoint inspectors to conduct investigations and outlines their powers.

Complaints and discipline

A person aggrieved by the conduct of a commercial agent or commercial sub-agent can make a complaint in writing to the chief executive. A breach of a code of conduct is a sufficient ground to commence disciplinary proceedings.

Chapter 13 of the Bill establishes the Property Agents and Motor Dealers Tribunal. The tribunal will consist of a chairperson and at least six other members. To be eligible to be a member, the person must be a lawyer with five or more years' experience, have business experience within one of the industries regulated by the draft Bill, have experience in business or finance, or have qualifications that make him/her suitable to represent community interests.

Under s. 438, the tribunal has the following jurisdiction:

- (a) to hear and decide disciplinary matters involving licensees and registered employees;
- (b) to hear and decide claims, other than minor claims, against the fund;
- (c) to review decisions of the chief executive in relation to minor claims;
- (d) to review decisions of the chief executive in relation to licensing and registration.

Section 483 outlines the grounds for commencing disciplinary proceedings. The grounds include:

- a breach of a code of conduct
- conviction of an indictable offence or an offence against this Act (draft Bill)
- an amount has been paid from the fund because the licensee or employee did, or omitted to do, something that gave rise to a claim against the fund
- assisting a person to obtain a licence fraudulently
- failure to comply with an order made by the Small Claims Tribunal, a court or the tribunal itself.

The following are grounds for disciplinary action against the licensee and registered employee (s. 483(1)):

- (h) for a licensee —
 - (i) the licensee is not a suitable person to hold a licence; or
 - (ii) the licensee has carried on, or is carrying on, business under a licence with someone who is not a suitable person to hold a licence; or
 - (iii) the licensee has, in carrying on a business or performing an activity, been incompetent or acted in an unprofessional way; or
 - (iv) the licensee has failed to ensure that the licensee's employed licensees or registered employees, or employees under the licensee's supervision—
 - (A) are properly supervised in the performance of their duties; or
 - (B) comply with this Act; or
 - (v) the licensee has failed to comply with a condition of the licensee's licence; or
 - (vi) the licensee is an executive officer of a corporation that the tribunal finds guilty of a disciplinary charge under section 514, or
 - (vii) if the licensee is a corporation —
 - (A) an executive officer of the corporation is not a suitable person to be an executive officer of a corporation; or
 - (B) an executive officer of the corporation is disqualified under this Act from being an executive officer of a corporation;

- (i) for a registered employee —
 - (i) the employee is not eligible to be employed as a registered employee; or
 - (ii) the employee has —
 - (A) in performing an activity of a licensee, been incompetent or acted in an unprofessional way; or
 - (B) performed an activity not authorised under the employee's employment authority.
- (2) The chief executive must not start a disciplinary proceeding against an executive officer under subsection (1)(h)(vi) if the chief executive is satisfied —
- (a) the act or omission relevant to the proceeding against the corporation was done or made without the officer's knowledge; and
 - (b) the officer could not, with reasonable diligence, have prevented the doing of the act or the making of the omission.

Through s. 514, the draft Bill allows the tribunal to make one or more of the following orders against a person found guilty of a disciplinary charge:

- (a) an order reprimanding the person;
- (b) an order that the person pay to the chief executive, within the time stated in the order, a fine of not more than 200 penalty units;
- (c) an order that the person's licence be suspended for the period stated in the order;
- (d) an order —
 - (i) if the person is the holder of a licence at the time the order is made — that the licence be cancelled; or
 - (ii) whether or not the person is the holder of a licence at the time the order is made — that the person be disqualified permanently, or for the period stated in the order, from holding a licence;
- (e) an order, for a licensed individual who is an executive officer of a corporation, that the individual be disqualified permanently, or for the period stated in the order, from being an executive officer of a corporation that holds a licence;
- (f) an order imposing conditions on, or amending or revoking the conditions of, the person's licence;

- (g) another order the tribunal considers appropriate to ensure the person complies with this Act.
- (2) The tribunal may not make an order under subsection (1)(d)(ii) disqualifying the person from holding a licence if the tribunal is satisfied that a court has, in relation to the matter giving rise to the disciplinary charge, declined to make an order under section 573(2) disqualifying the person from holding a licence after being asked to do so.

Provisions have also been made to allow the tribunal to make certain types of orders for claim hearings and review hearings.

PRIVATE INVESTIGATORS

Governing legislation

The private investigation industry is regulated through the Security Providers Act 1993. The Office of Fair Trading, within the Department of Equity and Fair Trading, is responsible for the administration of the Act and maintaining the register of licensed businesses/operators.

Legal definition of private investigator

Crowd controllers, security officers, security firms and private investigators are all classified as security providers. The Act defines 'private investigator' in the following terms:

- 6.(1) A private investigator is a person who, for reward, obtains and gives information about another person.

The term does not include a legal practitioner, accountant, insurer, insurance-adjustment agency or credit-reporting agent within the meaning of the Invasion of Privacy Act 1971.

A 'security firm' is defined as a person who, or partnership that, engages in the business of supplying, for reward, the services of crowd controllers, security officers or private investigators to other persons (s. 8).

Application and eligibility for a licence

Section 11 of the Security Providers Act specifies that, to apply for a licence, a person must:

- be 18 years or older
- have completed a training course approved by the chief executive of the Office of Fair Trading
- be an appropriate person to hold a licence.

Under s. 11(4), the chief executive can refuse to

grant a licence to an applicant on any of the following grounds:

- (a) that, in dealings in which the person has been involved, the person has
 - (i) shown dishonesty or lack of integrity; or
 - (ii) used harassing tactics;
- (b) that the person associates with a criminal in a way that indicates involvement in unlawful activity;
- (c) that the person has taken advantage, as a debtor, of the laws of bankruptcy;
- (d) that the person is or was a patient within the meaning of the **Mental Health Act 1974**;
- (e) that the person has been convicted of an offence.

The chief executive may also take into account the following provisions:

- (5) A person is not an appropriate person to hold a licence if the person, within 10 years of applying for a licence, has been convicted of —
 - (a) a disqualifying offence; or
 - (b) an offence that would be a disqualifying offence if committed in Queensland.

A disqualifying offence means an offence under the:

- **Weapons Act 1990** when it is punishable by imprisonment for one year or more
- **Drugs Misuse Act 1986** when it is punishable by imprisonment for one year or more
- **Criminal Code** when it is mentioned in the prescribed schedule (appendix V).

Section 12 allows the chief executive to make inquiries to determine if someone is an appropriate person to be granted a licence, or to determine if he/she continues to be an appropriate person. This Act also allows the chief executive to request the Commissioner of Police to provide a written report about a person's criminal history. Under the legislation, the Commissioner must comply with any such requests.

For a corporation to obtain a security firm licence, the chief executive must be satisfied that each person who is an officer of the corporation²⁹ is a suitable person as defined above. The licence must also specify which functions of a crowd controller, private investigator or security officer are permitted to be supplied by the corporation.

Licences are valid for up to one year and cost \$84.30.

The register of training courses shows that there are currently 99 approved training courses, with 15 tailored specifically to private investigation. To be approved, a training course must cover a number of basic topics (table 8.1).

Table 8.1 — Basic requirements for a private-investigator course

Role of the private investigator
Concept and methods of investigation
General investigative methodology and structure
Taking client instructions
Relevant structure and processes of law
The court system
The law as it applies to investigations
Providing advice and information to clients
Rules, policies and procedures relating to evidence
Human behaviour
Interview techniques
Sources of information
Locating and/or pursuing missing persons
Compilation of reports and statements
First-aid training

The majority of training providers come from the private sector.

The Director-General of the Department of Equity and Fair Trading has recently indicated that the training as described above is currently in the process of being phased out 'following the endorsement of competency standards in March 1996 by the Australian National Training Authority and the subsequent endorsement of the National Training Package for Asset Security — Security and Investigative Services (PRS98) ('the Training Package') in December 1998'. It was also indicated that a range of competencies from the Training Package will soon be selected and serve as minimum requirements for applicants to be eligible for a licence.

Licence renewal

Licensees must apply for renewal of their licence within the period starting one month before the licence ends and ending six months after the licence ends.

During renewal, background criminal-history checks may be performed on the applicant again.

Licence suspension, cancellation and refusal for renewal

The Security Providers Act 1993 (s. 21(1)) makes the following grounds for the suspension, cancellation or refusal to renew a licence:

- (a) the licence was obtained on the basis of incorrect or misleading information;
- (b) the licensee has contravened a condition of the licence;
- (c) the licensee has committed an offence against this Act;
- (d) the licensee, or another person required to be an appropriate person for the grant of the licence, is not, or is no longer, an appropriate person.

Being charged with a disqualifying offence is grounds for suspension or refusal to renew until the end of the proceeding for the charge. Through the Bail Act 1980, the court is empowered to impose a condition of bail that prevents a licensee from operating as a security provider.

Complaints and discipline

Part 3 (Inspectors) of the Security Provider Act allows the chief executive officer to appoint inspectors to conduct investigations. This part is similar in nature to the provisions described earlier for the draft Property Agents and Motor Dealers Bill 2000 in that it outlines the specific powers of inspectors.

NON-GOVERNMENT ASSOCIATIONS AND INSTITUTES

There are a number of non-government associations that offer products and/or services for professional development and networking for private investigator and/or commercial agents. It is not practicable to provide an exhaustive list of these organisations; however, four are discussed below by way of example:

- The Institute of Mercantile Agents (IMA) claims to be the only organisation representing the interests of commercial agents and private inquiry agents on a national basis. A critical goal of the IMA is the development and maintenance of an effective profession. To apply for membership, the applicant must agree to adhere to the Institute's Code of Ethics and the Code of Conduct.
- For small businesses and sole operators in Queensland, the Queensland Security

Association Inc. aims to provide services, products and networking opportunities. Clearly membership is for people classified as security providers, as defined by the Security Providers Act. To join the Association applicants must sign an agreement that they have read, understood and are willing to abide by the Association's Code of Ethics. The Association will cancel membership of a sole operator or business if there is evidence of conduct that breaches the Code (e.g. last financial year the Association removed two members). Also, there exist within Queensland a Security Industry Regulatory Council and a Police Security Liaison Board. Both try to deal with problems that arise within the Security Industry.

- The Australian Institute of Private Detectives is based in Sydney and was formed in response to the ICAC Inquiry in 1992. The Institute has a Code of Conduct that allows penalties of caution, reprimand, expulsion, fine and suspension to be imposed on members where there is evidence of a breach of any clause of the Code.
- The Australian Security Industry Association Limited (ASAIL) 'aims to lead and support the Australian security industry in the provision of security products and services to the Australian community'. The organisation was formed 'in 1969 as a national association with the express aim of becoming a self-regulatory body to ensure a high level of service for security users' (ASAIL web site, 20 July 2000).

It is not necessary to be a member of any of the above in order to hold a licence as a commercial agent or private investigator. Consequently, the ability of the above associations and similar associations to regulate the various aspects of the industry is limited. However, the mere existence of these types of associations, along with the requirement to adhere to codes of conduct, does help to improve integrity and professionalism within the industry.

CJC COMMENT ON INDUSTRY REGULATION

Although the CJC has recommended some increase in access to certain types of confidential information held by government agencies, it has not made recommendations that will entirely satisfy the industry. There is clear evidence that members of the industry have had access to information that they should not have been able

to obtain. This has been the experience in other jurisdictions. It would not be appropriate at this time to extend their access beyond that which has been recommended in this report. However, this should be reviewed when the effectiveness of the Property Agents and Motor Dealers Bill 2000 has been evaluated.

Commercial agents

The proposed Property Agents and Motor Dealers Bill 2000 is clearly a comprehensive document that considerably changes and improves the regulation of commercial agents in Queensland. In respect of the Bill, the CJC provided the Deputy Commissioner and Official Solicitor for the Office of Fair Trading with the comments outlined below. The Director-General of the Department of Equity and Fair Trading responded to the CJC comments, and her response is reported where appropriate.

1. A person is not suitable to hold a licence (s. 26(1)) or obtain registration as a registered employee (s. 82(1)) if the person is a person who has been convicted, in Queensland, or elsewhere, within the preceding five years, of a serious offence.

The CJC supports the wider definition of 'convict', as it appeared in schedule 3 of the draft Bill, meaning 'find guilty' or 'accept a plea of guilty'. This definition addresses the issue of those who are found guilty of an offence that renders them unsuitable to hold a licence but who have had no formal conviction recorded.

The Director-General has indicated that this definition of 'convict' has been amended to accord with other legislation administered by the Office of Fair Trading so that only recorded convictions will be considered. The CJC maintains its support for the original definition. The Director-General also argued that the new definition is aligned with the philosophy of the *Penalties and Sentences Act 1992*. This issue is further discussed on pages 103–4 in relation to the Security Providers Act.

The CJC considers that the definition of 'serious offence' in schedule 3 is too narrow. In particular, the disqualifying drug offence of 'trafficking in dangerous drugs' will only catch a limited class of drug offenders, and there are a number of other serious drug offences that should be included in the definition. For example, a person may supply significant quantities of dangerous drugs to someone else or be found in possession of a large quantity of dangerous drugs yet not have committed the offence of trafficking in dangerous drugs. The CJC also considers that the definition should include an attempt to commit a serious offence.

The Director-General has indicated that, while there is agreement that the above types of offences can be serious, their inclusion in the definition is not necessary because the chief executive can take them into consideration when determining the applicant's suitability to hold a licence or registration certificate. The CJC acknowledges that the chief executive has a residual discretion but nevertheless considers that this fails to resolve the inconsistency that certain offences result in automatic disqualification whereas other equally relevant and serious offences do not.

Paragraphs (a), (b) and (c) of the definition of serious offence use the words 'an offence involving' a certain type of conduct. While the CJC understands that the intention is probably to be over-inclusive (rather than under-inclusive) when defining this phrase, the effect may be quite the opposite. The word 'involving' is not generally used in offences under the criminal law. In interpreting this phrase, a court may read the word to mean, for example, an offence that includes (say) fraud as one of its elements. There are some offences that are quite serious but do not involve fraud or dishonesty as an element of the offence. Perhaps consideration can be given to the development of a schedule of offences that would fall within the definition of serious offence.

2. The chief executive must, when deciding whether a person is suitable to hold a licence (s. 28(1)) or obtain registration as a registered employee (s. 83(1)), consider a number of things.

The CJC recommends that a further consideration be whether the applicant has been convicted of official misconduct by a Misconduct Tribunal pursuant to the *Misconduct Tribunals Act 1997*. Official misconduct is defined in s. 32(1) of the *Criminal Justice Act 1989*. It is a lengthy provision and need not be repeated here. However, in essence it involves conduct of a public officer that is dishonest or not impartial or constitutes a breach of trust or concerns the misuse of information and is so serious as to constitute a criminal offence or a disciplinary breach that provides grounds for termination of employment.

3. The chief executive officer may ask the Commissioner of Police for a written report about the criminal history of any persons (s. 31(2) and s. 84(2)).

The CJC is of the view that, with one exception, when determining the suitability of a person to operate as a commercial agent or sub-agent it should be mandatory, not discretionary, for the Chief Executive to consider a written report from the

Commissioner of Police about that person's criminal history. To do otherwise risks a licence being granted to an unsuitable person, with consequent risks to the industry and the public generally.

The exceptional circumstance would be where it is known from other information that the applicant is an unsuitable person to hold a licence under s. 26(1). For example, it may be known that the applicant is an undischarged bankrupt or has admitted in the application to having been convicted of a serious offence within the last five years. In these circumstances, any further inquiry would be unnecessary.

Any costs associated with performing such checks can be offset by application fees.

The Director-General has commented that a discretionary provision was inserted because such checks are not performed on lower-risk applications, such as salesperson and sub-agent. It was also pointed out that 'given the volume of applications received, this has been a resourcing issue for both this department and Police. The recent decision to pass on the cost of performing these checks to this department without any budget supplementation has further exacerbated this situation.'

The CJC is sympathetic to the argument about budgetary constraints; however, it maintains that the force of its original submission (i.e. for criminal-history checks for applications or renewals of commercial agent or sub-agent licences) remains undiminished. Compliance with automatic exclusion on the basis of criminal history can only be effectively enforced by checking each application or renewal as a matter of course. The problem of cost must be solved by some other means (e.g. sharing costs, cost recovery from applicants, applying for additional funding) rather than by compromising the integrity of the application process.

4. An individual is eligible to obtain a commercial agent's licence only if the individual has the educational or other qualifications for a commercial agent's licence that may be prescribed under regulation (s. 44(1)(b)).

The CJC is very supportive of minimum educational and training qualifications as a precondition for the granting of licences. In the CJC's view, the absence of such a requirement under the present scheme has contributed to malpractice and unlawful conduct in the industry. The CJC urges the Department to prescribe such qualifications as a matter of urgency. The CJC is not aware of the standards or course content envisaged by the Department. As a result

of its experience, the CJC believes that there is a clear demand for instruction in the means by which commercial agents can lawfully obtain confidential government information.

Furthermore, continuing education by way of refresher courses should be a mandatory requirement for the renewal of a licence. For this reason, the CJC is concerned about s. 55(2)(d), which provides that the chief executive does not have to be satisfied that the licensee meets the eligibility requirements of an educational nature before renewing the licence. The CJC acknowledges that it is undesirable to require people renewing their licences to meet the same eligibility criteria as those who are applying for the first time; however, it does believe that there be some requirement of an educational nature.

5. A regulation may prescribe a code of conduct about commercial agency practice (s. 337).

The CJC is of the view that a code of conduct for commercial agents and sub-agents should be mandatory. The lack of such a code is a major regulatory deficiency in the commercial-agency industry. As the draft Bill suggests, a code should set out the professional standards required. In addition, in the absence of a code of conduct, a major ground for instituting disciplinary proceedings under s. 483(1) would not be available.

The Director-General has indicated that a draft code for commercial agents was developed in consultation with the industry. It was developed around ethical principles, which include respect for law and government, and respect for persons and integrity. It was commented by the Director-General that 'While this draft Code still requires refinement, the inclusion of such a Code in the new legislation will assist in addressing some of the concerns raised by your Commission.'

6. Grounds for starting disciplinary proceedings (s. 483(1))

Section 483(1)(a) provides that one ground for commencing disciplinary proceedings against a licensee is where the licensee has been convicted of an indictable offence or an offence against the Property Agents and Motor Dealers Act. The CJC is of the view that this ground is too narrow in that it excludes convictions for summary offences. While it is noted that there is provision for disciplinary proceedings to be commenced where a licensee is not a suitable person (s. 483(1)(h)(i)) it is preferable that a specific reference to convictions for summary offences be included in subparagraph (1)(a).

7. Transitional arrangement for existing licence-holders

The effect of s. 589 of the Act is to automatically licence those people who held licences under the previous Act upon the commencement of the Property Agents and Motor Dealers Act. This is understandable. However, the CJC has carefully considered s. 589(5), which provides that, where a person would not have been suitable for a licence under the Property Agents and Motor Dealers Act because of a matter or event which happened before the last licence was granted, renewed or restored, the matter or event may be disregarded for the purpose of renewal or restoration of the licence after the commencement of the new Act. If this provision is used, there will be existing licence holders who are entitled to remain in the industry although they would have been deemed unsuitable under the new scheme. The CJC initially considered a recommendation opposing the enactment of s. 589(5). In response, the Director-General has submitted that:

While your Commission's concerns, that there may be inappropriate persons allowed to remain in the industry, may have merit, there is a general reluctance by any government to retrospectively legislate for the removal of such persons from their licensed occupation.

Part of the rationale for this approach has been that these persons have set up their business operations based on their future compliance with legislated standards. To retrospectively remove that right is likely to create unnecessary hardship for the licensee and their employees.

The CJC is persuaded by the above submission and makes no recommendation opposing the transitional arrangement for existing licence-holders.

8. Continuous development forum

As recognised by the Minister for Fair Trading in her letter to stakeholders, the goal of modernising the law is 'to create greater flexibility in dealing with the evolving business environment', and the CJC is extremely supportive of the continuous-improvement approach being adopted. To complement the provisions of the draft Bill, the CJC suggests that a forum be established, consisting of various stakeholders (e.g. representatives of non-government associations, industry representatives, significant policy makers and researchers in the area, the QPS) to advise the Office of Fair Trading on professional-development initiatives and new methods of regulatory control. It is important that industry

participants be involved, be part of the regulatory process and have some degree of ownership of and participation in new policies, initiatives and changes to regulatory practices.

The above eight points outline the few comments that the CJC has made on the draft Bill. In relation to several of these issues, the CJC and the Office of Fair Trading hold different views on what is required to be detailed in legislation to ensure that the most comprehensive method of government regulation is established. As the draft Bill currently awaits debate in Parliament, the CJC recommends that its comments, as outlined above, be considered by Parliament when finalising the Bill.

RECOMMENDATION 8.1 — GOVERNMENT CONSIDERATION OF CJC COMMENTS ON THE DRAFT PROPERTY AGENTS AND MOTOR DEALERS BILL 2000

That the Queensland Government, which will soon debate the draft Property Agents and Motor Dealers Bill 2000, give serious consideration to the issues raised and the suggestions made within this report to further improve the regulatory control to be afforded by the new legislation.

Private investigators

As private investigators are, under legislation, considered security providers (along with crowd controllers, security officers and security firms), many of the research articles referred to in this section concern all categories of security providers, not just private investigators. Nevertheless, all security providers are regulated in the same way, so the concerns apply equally to each form of security provider.

Compared with the new regulatory system being proposed for commercial agents, the present system for security providers, including private investigators, is arguably weak. There is considerable agreement in the literature that much more can be done to regulate the security industry and that current strategies may not be adequate (the Community Law Reform Committee of the Australian Capital Territory 1995; Prenzler & Sarre 1998; Prenzler, Draper & Harrison 1996; Sarre 1994, 1998; Swanton 1993). Similarly the NSW Department of Consumer Affairs in 1993 released *Review of private investigation industry: A discussion paper*, which also examined the regulatory system's deficiencies.³⁰

Prenzler, Baxter & Draper (1998) argued that the Qld Security Providers Act was an important step in the right direction but that a number of

deficiencies impair its capacity to upgrade the security industry to the required standard. Prenzler & Sarre (1999) conducted a survey of security legislation and regulatory strategies in Australia and concluded that a unified national system, with implementation of more proactive forms of compliance monitoring and professional development, was needed to improve the operation of the security industry. They also commented that Queensland has very limited coverage of the security industry with regard to licensing (e.g. control-room operators, bodyguards, installers and repairers do not require a licence to operate in Queensland). A survey conducted in Queensland with members of the security industry found that the majority of respondents did not believe that the Security Providers Act had removed 'shonky operators' and thought licensing should be extended (Prenzler & Hayes 1999).

Different models of regulation are discussed in the literature, but the favoured approach is some kind of co-regulation. In 1995 the Community Law Reform Committee of the ACT recommended:

- a co-regulatory body to provide advice to government on issues concerning the industry, to consider disciplinary matters and to develop training policy
- a code of practice that addresses the obligations of employers, the price and quality of services, confidentiality of personal information, the standard of equipment and the qualifications and employment of staff.

It was also pointed out that purely legislative schemes for regulation require an administrative infrastructure involving licensing and compliance elements. The financial costs of regulation need to be absorbed through the community (e.g. by funding out of general revenue), by industry (e.g. by means of an industry-specific levy) or by a mixture of the two funding sources.

The Queensland Security Association has made it clear that they believe there are gaps and deficiencies in the current Queensland legislation. The Association has submitted to government on several occasions that there is a need to amend the current legislation to improve industry regulation. Suggestions in this submission include:

- development of a code of ethics that is applicable to all security providers
- changes to clearly define the terms 'security officer', 'investigator', 'product/service provider' and 'training provider'

- requirements for training providers to be licence-holders
- the establishment of traineeships
- the establishment of a control board with representation from stakeholders (e.g. police, industry representatives) to oversee industry regulation
- the empowerment of the control board to direct persons to undertake a course of education as determined by the Board
- clearly defining 'unlawful representation as a security provider'
- the establishment of a Consumer Complaints Tribunal to receive complaints against security providers
- the creation of a Mutual Indemnity Fund.

Consideration of the legislation and industry regulation suggests that there are a number of problematic areas with the current regime, and that there is an urgent need to review the practices in Queensland. It is well beyond the scope of this report to conduct such a review, particularly as private investigators, the industry group of interest to this Inquiry, are only one form of security provider. The problems and deficiencies that have been identified in the regulation of private investigators are equally apparent in the regulation of security officers, crowd controllers and security firms. Other stakeholders, such as the QPS, the Department of Equity and Fair Trading, the Office of Fair Trading and industry experts (e.g. significant researchers and policy-makers in the field) should be part of any review process. In determining best practice, consideration should be given to models in other States, Territories and countries, as well as to the draft Property Agents and Motor Dealers Bill 2000.

A review of industry regulation and of the Act would require adequate representation from each of the four categories of security providers.

The scope of a review should include, but not be limited to, the:

- adequacy of the definition of 'security provider'
- adequacy of the licensing system and exclusion criteria
- level of prerequisite and ongoing training requirements, and alignment with any existing national competencies and ongoing training-and-development processes
- suitability of the current complaints and discipline processes.

It should also be noted that the Director-General has recently indicated that the Government intends to conduct a review of the *Security Providers Act 1993*.

In recent correspondence from the Director-General, it has been emphasised that there has been correspondence between the Minister of Fair Trading and the Minister for Police on whether or not the *Security Providers Act* should stay within the Fair Trading portfolio. The Director-General commented: 'Preliminary discussions have been held at senior officer level to commence an investigation of the appropriateness of the transfer of administrative responsibility to Police. This approach would align Queensland with the major States around Australia where the licensing of security officers and private investigators is undertaken by Police.'

The CJC believes that there is merit in the argument that the QPS may be better positioned to take responsibility for the *Security Providers Act*. Clearly there needs to be careful consideration of all of the issues regarding location before such a decision is made.³¹ It may be appropriate to consider that debate as part of the broader review of industry regulation recommended in this report.

RECOMMENDATION 8.2 — GOVERNMENT REVIEW FOR THE BETTER REGULATION OF THE SECURITY INDUSTRY

That the Queensland Government commence a review of the *Security Providers Act 1993* and industry regulation within the next twelve months. The review should aim to develop legislation to provide a regulatory environment that is comprehensive and that ensures that the professionalism and integrity of the security industry are strengthened.

One matter of immediate concern to the CJC is that the present *Security Providers Act 1993* allows exclusion on prescribed disqualifying offences to be waived if no conviction is recorded when a person is found guilty of an offence.

Section 12(2) of the *Penalties and Sentences Act 1992* provides:

In considering whether or not to record a conviction, a court must have regard to all circumstances of the case, including—

- (a) the nature of the offence; and
- (b) the offender's character and age; and
- (c) the impact that recording a conviction will have on the offender's —
 - (i) economic or social wellbeing; or
 - (ii) chances of finding employment.

These provisions are designed to protect the individual from excessive punishment. However, there may be occasions where the conduct for which someone was brought before the court calls into question that person's integrity and capacity to perform his/her duties appropriately. There has been considerable comment on whether, for some types of offences, the most important criterion is whether the person is found guilty or not, rather than whether a conviction was recorded or not. Examples of possible classes of offences where a guilty verdict may call into question a person's integrity and suitability to operate as a security provider are assault, and drug and weapon offences. As shown in table 8.2, there is a fair likelihood that a first- and perhaps even second-time offender may not have a conviction recorded.

While it is necessary for magistrates and judges to

Table 8.2 — Number of charges at all court locations for all lower courts: 1.7.98 – 30.6.99

OFFENCE TYPE	CONVICTION RECORDED	NO CONVICTION RECORDED
Major assault	1254	356
Minor assault	7122	2793
Possession or use of drugs	7107	4837
Dealing and trafficking in drugs	432	222
Manufacturing and growing drugs	819	572
Other drug offences	6253	4270
Weapons offences	2178	1026

Source: Office of Economic and Statistical Research (OESR), Queensland Government

Notes: 1. Does not distinguish between first-time offender and re-offender

2. Number of offences does not equate to number of individuals. Individuals may be charged with multiple offences.

determine the harshness of the penalties imposed for an offence, it is equally important that the authority responsible for regulating the security industry can discharge its duties effectively. One important duty is to ensure that individuals of questionable integrity have their licence cancelled. It is assumed that the disqualifying offences listed in the Security Providers Act were selected because they would bring into question a person's integrity and his/her suitability to hold a security licence; in this case, it is the guilt of the person that is important, not whether a conviction was recorded or not.

Clearly, it is necessary to amend the Security Providers Act to allow the chief executive discretion to determine the suitability of an applicant or current security operator based on comprehensive knowledge of the person's background, character and integrity. This cannot be achieved if the executive officer cannot exclude a person who has committed a disqualifying offence but had no conviction recorded. Discretionary decision-making on suitability should be recorded to ensure consistency in decision-making over time.

This should serve as an interim measure until the review of the legislation and industry regulation is complete. Part of that review should be to assess the adequacy of the current schedule of disqualifying offences and whether the disqualifying period of ten years is appropriate.

It should be noted that the position of the Department of Equity and Fair Trading is that the legislation should remain in its current form. The Director-General has submitted that these issues 'should be approached from a whole of government policy perspective rather than targeting legislation that regulates the activities of private investigators and commercial agents operating in a commercial environment'. The view of the CJC is that integrity concerns are more relevant in some occupations. For example, the **Criminal Law (Rehabilitation of Offenders) Act 1986** permits the disclosure of full criminal history (i.e. whether conviction is recorded or not) for employment in particular occupations or areas of government (e.g. Corrective Services, Education Queensland).

The CJC is of the view that the private investigator and commercial agent industries are two industries where integrity issues are similarly important.

RECOMMENDATION 8.3 — AMENDMENTS TO THE SECURITY PROVIDERS ACT 1993

8.3.1 That, as a matter of urgency, the Security Providers Act 1993 be amended

to allow the chief executive officer to consider the suitability of an applicant or current licence-holder where that person has been found guilty of a disqualifying offence.

8.3.2 That, as part of the government review of legislation and industry regulation, the suitability of current disqualifying offences and the disqualifying period be reconsidered.

CONCLUSION

For both the commercial agent and private investigator industries, the current regime of government regulation is not sufficient to ensure even the minimum level of professionalism and integrity.

During the writing of this report, it came to light that the Office of Fair Trading has, for some time, been developing new legislation that will significantly change the regulation of the commercial agent industry. The CJC was able to consider the draft Property Agents and Motor Dealers Bill 2000, which was released for public consultation on 26 July 2000. The CJC provided comments to the Office of Fair Trading. A draft of this report was also provided, and the Director-General of the Department of Equity and Fair Trading responded with some comments. Where appropriate, the comments have been incorporated into this report.

The comments of the CJC and the response from the Director-General are outlined through pages 99–101. The CJC has recommended that the Queensland Government, which is currently considering the draft Bill, give serious consideration to the suggestions made within this report to further improve the regulatory control afforded by the draft Bill.

Government regulation of the private investigator industry is considerably weaker than what is being proposed for the commercial agent industry. A review of the literature showed general consensus that much more could be done to better regulate the industry to bring it up to the required standard. Suggestions for improvement include a mandatory code of conduct, the establishment of a complaints-receiving body, more stringent training requirements and changes to criteria for automatic exclusion. It has been recommended that the Government review the **Security Providers Act 1993** with a view to tightening regulation to improve the industry standards to the requisite level for ensuring professionalism and integrity.

INFORMATION PROTECTION AND THE LAW

The CJC's investigations focused on:

- police officers unlawfully accessing confidential government-held information
- police officers unlawfully releasing confidential government-held information
- efforts by those outside the QPS to unlawfully obtain confidential government-held information.

The purpose of this chapter is to discuss the legislation that applies to the improper use of information held by the State Government and, more particularly, by the QPS.

Where necessary, recommendations are made to improve the legislative provisions to allow disciplinary charges and/or criminal charges to be preferred.

The final section of the chapter considers the broader issue of information protection and privacy legislation. This discussion includes comments from stakeholders regarding the adequacy of the legislation.

UNLAWFUL ACCESS TO CONFIDENTIAL GOVERNMENT-HELD INFORMATION BY MEMBERS OF THE QPS

Evidence was obtained during this Inquiry of authorised QPS computer-users accessing confidential government-held information without an official work-related purpose. This type of conduct is clearly unacceptable and represents an infringement of the rights of those individuals about whom confidential information is held by the QPS and Queensland Transport.

The Code of Conduct and chapter 4 of the QPS Administration Manual provide that improper access to the police computer system is misconduct. Misconduct is defined in the PSAA as conduct that:

- (a) is disgraceful, improper or unbecoming an officer; or
- (b) shows unfitness to be or continue as an officer; or
- (c) does not meet the standard of conduct the community reasonably expects of a police officer.

However, it is not an offence under any Act for a person who is an authorised user to improperly access confidential government information held by the QPS.

The Australian Privacy Charter Council was of the view that there was a need for the legislation to combat this behaviour. Through its representative at the CJC's hearing, it submitted that browsing should be an offence:

Another recommendation we would have would be that it should not be just disclosure of confidential information that should be an offence but the mere browsing of a computer system should be detectable and should be made an offence if it's obvious that that's occurring for non-authorised reasons. (CJC unpub., p. 768)

In chapter 6 ('Improving Information Security in the QPS'), the CJC recommended that an order be promulgated that prohibits accessing classified information on the QPS computer system without adequate justification. The existence of such an order will ensure that QPS management is in a position to take disciplinary action against any member who cannot demonstrate official work-related reasons for their computer access.

Given the above provision, the CJC is of the view that it is not necessary to make it an offence under the PSAA to improperly access classified computer information.

UNLAWFUL RELEASE OF CONFIDENTIAL AND/OR PERSONAL INFORMATION

A range of Queensland laws prohibit the release of information.

Section 10(1) of the PSAA makes it an offence for a member to improperly release confidential information:

(1) Any officer or staff member or person who has been an officer or a staff member who, except for the purposes of the Police Service, discloses information that —

(a) has come to the knowledge of, or has been confirmed by, the officer or staff member or person through exercise, performance or use of any power, authority, duty or access had by the officer or staff member or person because of employment in the service; or

(b) has come to the knowledge of the officer or staff member or person because of employment in the service;

commits an offence against this Act, unless —

(a) the disclosure is authorised by the commissioner under section 10.2; or

(b) the disclosure is made under due process of law; or

(c) the information is not of a confidential or privileged nature; or

(d) the information would normally be made available to any member of the public on request.

Maximum penalty — 100 penalty units.³²

(2) In prosecution proceedings for an offence defined in subsection (1), it is irrelevant that information of the nature of that disclosed had also come to the defendant's knowledge otherwise than in a manner prescribed by subsection (1).

There are also provisions in the Police Powers and Responsibilities Act 2000 and the Juvenile Justice Act 1992 that make it an offence to release improperly certain classes of protected information (e.g. information obtained through the use of a listening device, or the name of a juvenile who makes a community-conference agreement).

The Act makes it a disciplinary offence for an employee or appointee of any unit of public administration in Queensland to misuse information:

32.(1) Official misconduct is — ...

(c) conduct that involves the misuse by any person of information or material that the person has acquired in or in connection with the discharge of his or her functions or exercise of his or her powers or authority as the holder of an appointment in a unit of public administration, whether the misuse is for the benefit of the persons or another person;

and in any such case, constitutes or could constitute —

(d) in the case of conduct of a person who is the holder of an appointment in the unit of public administration — a criminal offence, or a disciplinary breach that provides reasonable grounds for termination of the person's services in the unit of public administration.

Finally, the Criminal Code makes it an offence for a former or current public officer to publish or communicate secret government information:

85. A person who is or has been employed as a public officer who unlawfully publishes or communicates any information that comes or came to his or her knowledge, or any document that comes or came into his or her possession, by virtue of the person's office, and that it is or was his or her duty to keep secret, commits a misdemeanour.

Maximum penalty — 2 years imprisonment.

More generally s. 87(1) of the Criminal Code provides that 'it is an offence for a person who is employed in the public service, and charged with the performance of any duty by virtue of such employment or office, not being a duty touching the administration of justice, to corruptly receive or agree to receive a benefit on account of an act done by that person in the discharge of their duties'. The entire section provides for the offence of official corruption as follows:

87.(1) Any person who —

(a) being employed in the public service, or being the holder of any public office, and being charged with the performance of any duty by virtue of such employment or office, not being a duty touching the administration of justice, corruptly asks for, receives, or obtains, or agrees or attempts to receive or obtain, any property or benefit of any kind for himself, herself or any other person on account of anything already done or omitted to be done, or to be afterwards done or omitted to be done,

by the person in the discharge of the duties of the person's office;

is guilty of a crime, and is liable to imprisonment for 7 years, and to be fined at the discretion of the court.

Section 121(1)(a) creates an offence similar to that created by s. 87, but concerns corrupt conduct by public servants (which by definition includes police officers) whose duties of a non-judicial kind involve the prosecution, detention or punishment of offenders.

These latter two provisions of the Criminal Code could be applied in circumstances where, for example, a public officer corruptly received a benefit for providing confidential information in the discharge of his or her duties of office.

The CJC is of the view that the above provisions adequately address the improper release of confidential information by members of the QPS. More generally, the provisions under the Act and the Criminal Code are satisfactory insofar as public-sector employees are concerned.

UNLAWFULLY OBTAINING CONFIDENTIAL PERSONAL INFORMATION

A number of legislative provisions in Queensland prohibit people from seeking to obtain some advantage by giving a benefit to a police officer or any other public official.

Section 10.20(1) of the PSAA creates an offence of 'Bribery or corruption of officers or staff members'. Broadly speaking, the section prohibits a person from corruptly giving a benefit to any officer or staff member of the QPS with a view to influencing the officer or staff member in the execution of his or her duty. In particular, s. 10.20(1)(c) provides:

10.20(1) A person who corruptly gives to, confers on, or procures for any officer or staff member property or a benefit of any kind, or offers, promises or agrees to do so with a view to . . .

(c) the officer or staff member using or taking advantage of the officer's or member's position in the Police Service to facilitate commission of an offence, or to provide the person with any information, service or advantage whether or not the person would otherwise be entitled thereto;

commits an offence against this Act.

Maximum penalty — 100 penalty units.

Reference has previously been made to s. 87(1)(a) of the Code, which concerns corrupt conduct by a public official. Section 87(1)(b) creates an offence in respect of the person who gives the benefit to the public official. For example, this charge could be preferred against someone who corruptly confers a benefit upon a public officer in return for the official's providing confidential information in the discharge of their duties of office. The section provides:

87.(1) Any person who —

(b) corruptly gives, confers, or procures, or promises or offers to give or confer, or to procure or attempt to procure, to, upon, or for, any person employed in the public service, or being the holder of any public office, or to, upon, or for, any other person, any property or benefit of any kind on account of any such act or omission on the part of the person so employed or holding such office;

is guilty of a crime, and is liable to imprisonment for 7 years, and to be fined at the discretion of the court.

Similarly, s. 121(1)(b) of the Criminal Code creates an offence in respect of the person who gives the benefit to the public servant whose duties are of a non-judicial kind involving the prosecution, detention or punishment of offenders.

In simple terms, the provisions relating to bribery under the PSAA and official corruption under the Criminal Code require a benefit to be given to the public official before an offence can be inferred. This is one of the reasons that offences of this kind are so notoriously difficult to prove to the requisite standard. Benefits may take many forms, not merely monetary, and are often difficult to discover.

While there are examples of police officers providing such information to people outside the QPS in return for a benefit (previous operations of the CJC are proof of that), during the course of the present Inquiry there was no evidence of any benefit having passed from a person receiving the information to the officers who provided it. Information was frequently provided because of a relationship or friendship that had been established between the police officer and the person seeking the information. At the Nerang Police Station, officers provided the information because it appeared to be practice to do so. In the absence of proof of a benefit passing to the police officer, the only evidence available to the CJC was of a number of people being in the possession of QPS information. However, it is not

an offence under Queensland legislation to be in possession of confidential government-held information.

Similar legislative inadequacies were observed during the ICAC Inquiry (1992a) and it was concluded that:

Protected government information should be regarded as a prohibited commodity, like proscribed drugs or stolen goods. It should be an offence, not only for public officials to release it, but for others to buy or sell or otherwise deal in or handle it, or to disseminate it in any other way, without authority ... and a reverse onus of proof once unexplained possession or handling is established. (p. 171)

In their submission, the QPS also discussed the problem and suggested legislative amendments to deal with it:

No provision exists which creates an offence for a person to unlawfully receive or obtain information or benefit from information unlawfully obtained.

The Service believes that the following legislative change would act as a deterrent ...

- that the Police Service Administration Act or the Criminal Code be amended to include an offence for the unlawful possession, procurement, release or access of information by any person (including attempts, in respect of the Police Service Administration Act). (QPS submission 2000, p. 16)

In the CJC's view, the present legislative regime does not deal adequately with the issue of people outside the QPS being unlawfully in possession of confidential government-held information obtained from police officers and other members.

However, this inadequacy goes beyond just the unlawful possession of QPS data. Although the CJC's investigations related to information provided by police officers, many of the requests were in respect of information that is available on the motor-vehicle registration database owned by Queensland Transport. This database is made available to police but is similarly accessible by a large number of Queensland Transport employees. It is conceivable that a private investigator may also attempt to unlawfully obtain information through sources in that Department.

Furthermore, the ICAC Inquiry (1992a), which was a broader investigation into the unauthorised release of government information, found that 18 employees of the NSW Department of Motor

Transport or the Roads and Traffic Authority had engaged in corrupt conduct in connection with the illicit trade in information.

The lesson to be learned from the ICAC Inquiry, and one that logic alone suggests, is that there is a risk that any public-sector employee who has access to confidential government information will be targeted by those unlawfully seeking that information.

The CJC's Inquiry concerned misconduct on the part of QPS officers. It did not extend to the provision of information by public-sector employees elsewhere.

In the main the information was of a personal nature — that is, information such as a person's address or telephone number, criminal-charge record and the like.

In the CJC's view, legislation should be developed that prohibits people from obtaining or trying to obtain from government agencies personal information about other people, however it is held. The CJC is not in a position to assess whether any prohibition should be wider and apply to accessing confidential government information generally.

The proposed legislation must include a requirement for dishonesty on the part of the person seeking the information, or his/her knowledge that it is confidential. Otherwise it may capture innocent and not unreasonable requests for information, access to which is nevertheless restricted. For example, the legislation may provide that the person requesting the information knew or ought reasonably to have known that the information was confidential.

RECOMMENDATION 9.1 — MAKING IT AN OFFENCE TO OBTAIN OR TRY TO OBTAIN FROM GOVERNMENT RECORDS ANY CONFIDENTIAL INFORMATION ABOUT ANY OTHER PERSON, HOWEVER IT MAY BE HELD.

That consideration be given to the creation of an offence that prohibits people from obtaining or trying to obtain from government records any confidential information about any other person, however it may be held. The proposed legislation must include a requirement for dishonesty on the part of the person seeking the information, or his/her knowledge that the information is confidential.

THE ISSUE OF PRIVACY

Some of the recommendations made in the preceding sections represent specific legislative solutions to some of the problems uncovered

during the Inquiry. However, as discussed in chapter 2 ('The Central Issues'), there is also a trend toward establishing legislation designed to protect privacy because of the increased risks associated with computerised information systems. These systems allow efficient collection and dissemination of information but also put at risk the confidentiality of information and the privacy of the individuals in respect of whom, and from whom, information is collected.

In response to the matters revealed during this Inquiry, the Australian Privacy Charter Council and the Council for Civil Liberties both made a submission and appeared before the CJC during the non-investigative hearings. The Privacy Council was of the view that current Queensland privacy provisions are inadequate. It suggested that the most appropriate response to the issues uncovered during this Inquiry would be the introduction of privacy legislation:

It reinforces the urgent need for State privacy law, as recommended by the Queensland Parliament's Legal and Constitutional and Administrative Review Committee in its 1998 Report *Privacy in Queensland*, and accepted in principle by the State government. (APCC submission 2000, p. 1)

The Privacy Council also agreed that there needs to be a balance between legitimate public need for information and the need for the privacy of information.

The Council for Civil Liberties also argued that the privacy provisions in Queensland are inadequate:

This then brings me to my second issue which is the complete lack of privacy protection in Queensland at a State Government level. Even though, at the moment, the Federal Government is drafting legislation, which will cover the private sector to supplement their Government section legislation which has been in existence since the 1980s, even when fully drafted and passed that will not affect State Government or State Government entities so we still need separate legislation that will cover that.

At the moment there are no civil or criminal remedies for ordinary citizens whose privacy has been breached as a result of the misuse of the police service database. (CJC unpub., pp. 820–21)

As discussed in chapter 1, the Queensland Government is in the process of reviewing its position with regard to information privacy.

Considering its recent investigations in this area, the CJC is of the view that, when reviewing its position on information privacy, the Queensland Government should revisit the recommendations contained in the LCARC report. In particular, further consideration should be given to the introduction of a Privacy Act, based on the Commonwealth model, that contains information-privacy principles relating to personal information collected and held by Queensland Government departments and agencies.

The Commonwealth legislation not only provides a sound model but can also be considered to represent the national standard in privacy. As jurisdictions and governments share more information, particularly personal information about individuals, it is critical that legislation and policies are consistent between States, Territories and the Commonwealth. The importance of consistency was also emphasised in the report of the ICAC Inquiry (1992a):

There is little point in prohibiting in one State, practices which are permitted in another. In Australia, the goal should be not just consistency, but uniformity. And it should extend beyond legislation governing computers, to legislation governing the handling and transfer of government information generally. (p. 172)

RECOMMENDATION 9.2 — GOVERNMENT RESPONSE TO THE EMERGING ISSUES OF PRIVACY AND INFORMATION PROTECTION

That the Queensland Government, when reviewing its position on information privacy, revisit the recommendations made in the report of the Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland*, and in doing so give further consideration to the introduction of a Privacy Act based on the Commonwealth model.

CONCLUSION

The final issue revealed during the Inquiry was with regard to legislation. The first area relates to provisions within legislation that make it an offence for the behaviour observed during this investigation to be a criminal offence. The CJC was satisfied that legislative provisions for the improper release of confidential government information are adequate. On the issue of improper access to confidential government information by members of the QPS, it was recommended in chapter 6 ('Improving Information Security in the QPS') that the Commissioner of Police promulgate an order prohibiting unauthorised access to confidential

government information. Such an order would provide the necessary grounds on which to commence disciplinary action against a member who cannot demonstrate an official police reason for accessing classified information. The CJC did not consider it necessary to make improper access to computer systems by authorised members a criminal offence.

It was noted during this Inquiry and the ICAC Inquiry (1992a) that legislation was inadequate for prosecuting the individuals who attempt to procure, receive, obtain or possess classified government information when a financial benefit paid to the public-sector employee in exchange cannot be demonstrated (if it can be demonstrated, the individual can be charged with official corruption or a similar offence). This was particularly the case for end-users such as the financial institutions and legal firms, who were one step removed from the initial transaction between the member of the QPS and the private investigator. To handle this issue, the CJC has recommended that consideration be given to the creation of an offence that prohibits people from obtaining or trying to obtain from government records any confidential information about any other person (whatever the storage medium). The proposed legislation must include a requirement for dishonesty on the part of the person seeking the information, or his/her knowledge that the information is confidential.

The final issue, which received considerable attention in the public submissions, was that of privacy legislation. The report gave a brief outline of the emerging trend toward privacy legislation both nationally and internationally. The issue of privacy is not new in Queensland; in 1998 the LCARC released its report *Privacy in Queensland* and recommended that privacy legislation and a privacy commissioner be introduced. The current Government is reviewing its position on privacy and it is recommended that, as part of that review, the Government revisit the LCARC report and, in doing so, give further consideration to the introduction of a Privacy Act based on the Commonwealth model.

KEEPING THE ISSUES ON THE AGENDA

The objective of this report has been to identify, discuss and propose solutions for the issues of concern that were revealed during the Inquiry. As noted in chapter 2, there were three central issues that emerged and consequently shaped the structure of this report:

- information security
- the market for information and the intermediaries who facilitate information exchange
- legislation to protect information.

The first section of this chapter provides the concluding comments on each of these central issues.

This Inquiry was concerned with the conduct of members of the QPS. However, there is an important lesson here for all government departments and agencies that are responsible for the storage and protection of confidential government information. The next section of this chapter is concerned with describing the lessons to be learned from this Inquiry, and which have application to government more generally.

The chapter concludes with a discussion of how the CJC will follow-up on the implementation of recommendations made in the report.

FINAL COMMENTS ON THE THREE CENTRAL ISSUES

Information security

Management of information security is becoming an increasingly high priority for organisations. This is not surprising given that information is well recognised as a valuable asset. The advent of information technology has resulted in significant increases in the efficiency of information systems; this technology has also facilitated open communication systems and provided many individuals with immediate access to information that allows them to perform their duties more effectively.

With these rapid advances has come greater risk. This risk has been made even greater because of the lag in technologies capable of dealing with those risks and the delay by organisations, particularly government entities, in recognising the need to have strong information-security management. This Inquiry observed instances of members of the QPS:

- improperly accessing the computer systems, in particular the POLARIS and QPS System, for reasons unrelated to their official police duties
- improperly releasing information that was of a classified and personal nature to unauthorised third parties
- committing this type of misconduct with the awareness that their conduct was improper and against QPS policy
- performing transactions under a previous user's identification (where the previous user had left the terminal unattended and had failed to log out).

In assessing the QPS information security management system, all of the following were considered:

- the Australian and New Zealand Standard on Information Security Management (AS/NZS 4444.1:1999) in combination with a review of the current literature on best practice
- the issues raised through public submissions and presentation of evidence
- the experience of previous CJC investigations
- the lessons to be learnt from other jurisdictions, particularly the NSW Police Service
- the final comments and submission made by the QPS.

This report has made recommendations that represent both an organisational and a technological response to the issues raised. A significant number of recommendations have

been made to 'close any gaps' in policy and procedure (e.g. policy to prohibit leaving open computer terminals unattended, proper disposal of paper copies of in-confidence material, and mandatory recording of reasons for transactions). It has also been recommended that the location of the ISS be reviewed, giving consideration to its placement within the ESC. Technological recommendations for the development of features such as 'alert' monitoring to improve detection systems were also made. Finally, it has also been recommended that the QPS commence a program of systematic and ongoing internal audit on reasons for transactions, with both random and targeted components. This will allow the Service to be proactive in monitoring and detecting this type of misconduct.

The market for information and the intermediaries who facilitate information exchange

The observations made during this Inquiry were not very different from those made during the ICAC Inquiry (1992a). In the majority of instances, this type of misconduct occurred in response to an information request from an unauthorised third party. It became apparent that private investigators and commercial agents often serve as the information broker, who obtains information on behalf of clients, the majority of whom are private-sector businesses.

Of particular concern to the CJC are the regulatory requirements that have a legislative base. For both the commercial-agent and private-investigator industries, the current regime of government regulation is not sufficient to ensure even the minimum level of professionalism and integrity.

During the writing of this report, it came to light that the Office of Fair Trading has, for some time, been developing new legislation that will significantly change the regulation of the commercial-agent industry. The CJC was able to consider the draft Property Agents and Motor Dealers Bill 2000, which was released for public consultation on 26 July 2000. The regulation of the commercial-agent industry is significantly improved through the draft Bill. The CJC provided comments (outlined on pages 99–101) to the Office of Fair Trading, to which the Director-General of the Department of Equity and Fair Trading responded. On some issues there was a divergence of opinion between the two organisations, and it has been recommended that the Government consider the issues outlined in this report during the debate on the draft Bill.

Government regulation of the private-investigator industry is considerably weaker than what is

being proposed for the commercial-agent industry. A review of the literature showed general consensus that much more could be done for better regulation of the industry and to bring it up to the required standard. Suggestions for improvement include a mandatory code of conduct, the establishment of a complaints-receiving body, more-stringent training requirements and changes to criteria for automatic exclusion. This report has recommended that the Government review the **Security Providers Act 1993** with a view to tightening regulation to improve the industry standards to the requisite level to ensure professionalism and integrity.

Legislation to protect information

The other concern revealed during the Inquiry was with regard to legislation. The first area relates to provisions within legislation that make it an offence for the behaviour observed during this investigation to be a criminal offence. The CJC is satisfied that legislative provisions governing the improper release of confidential government information are adequate. On the issue of improper access to confidential government information by members of the QPS, it was recommended in chapter 6 ('Improving Information Security in the QPS') to make it an order of the Commissioner to prohibit unauthorised access to confidential government information. Such an order provides the necessary grounds to commence disciplinary action against a member who cannot demonstrate an official police reason for accessing classified information. The CJC did not consider it necessary to make improper access to computer systems by authorised members a criminal offence.

It was noted during this Inquiry and the ICAC Inquiry (1992a) that legislation was inadequate for prosecuting individuals who attempt to procure, receive, obtain or possess confidential government information when a financial benefit paid to the public-sector employee in exchange cannot be demonstrated (if it can be demonstrated, the individual can be charged with some type of bribery offence). This was particularly the case for end-users such as financial institutions and legal firms, who were one step removed from the initial transaction between the member of the QPS and the private investigator. Correspondence between private-sector businesses and the private investigator showed both the requests for and the provision of information that could not have been obtained by legally sanctioned means. To handle this issue, the CJC has recommended that consideration be given to the creation of an offence that prohibits people from obtaining or trying to obtain, from

government records, confidential information about any other person, however it is held. The proposed legislation must include a requirement of dishonesty on the part of the person seeking the information, or his/her knowledge that the information is confidential.

One issue that received considerable attention in the public submissions was that of privacy legislation. The report gave a brief outline of the emerging trend toward privacy legislation both nationally and internationally. The issue of privacy is not new in Queensland. In 1998 the LCARC released its report *Privacy in Queensland* and recommended that privacy legislation and a privacy commissioner be introduced. The current Government is reviewing its position on privacy, and this report recommends that, as part of that review, the Government revisit the LCARC report and in doing so give further consideration to the introduction of a Privacy Act based on the Commonwealth model.

THE LESSONS FOR ALL GOVERNMENT DEPARTMENTS AND AGENCIES

This investigation was initiated by a complaint that members of the Nerang Police Station were improperly accessing and releasing confidential information from the QPS computer systems. Consequently the focus of this report has been on information-security management within the QPS, particularly as it relates to the computer systems. The conduct of the subject officers provided a clear indication of where some accountability systems were lacking. A review of the information security systems after the public hearing identified further areas for improvement.

It would be unfair to suggest in this report that information-security management within the QPS is any less than that typically seen in other jurisdictions or other areas of government. Submissions and comments by representatives of Victoria Police, the NSW Police Service, the NSW Ombudsman and the South Australian Police Service reported similarly designed information-security systems characterised by similar problems. The QPS, in implementing the recommendations of this report, will tackle the common problems and concerns revealed during this Inquiry.

While this report was principally about the QPS, the issues may well be the same for other government departments and agencies that have access to confidential government information for which there may be an illicit market. It may not always be that such markets are restricted to confidential information of a personal nature; for example, a private-sector business may be quite

willing to purchase information on the tender bid of a competitor for a public-sector contract.

Each unit of public administration should consider:

- the extent to which its information-security management systems adhere to the best practice model prescribed in the Australian and New Zealand Standards on Information Security (AS/NZS 4444.1:1999 and 4444.2:2000) and the Information Security Risk Management Guidelines (HB 231: 2000)
- how comfortable the Minister or CEO would be that all the practicable steps to ensure that information security had been taken, should the agency find itself at the centre of an inquiry or media interest on release of information
- the extent to which conduct of the kind observed during this Inquiry can be detected and productively investigated under current accountability systems.

Given the rapid changes and innovations in information systems and information technology, it is essential that government, in particular, as a holder of vast amounts of personal information, aims to be progressive in its approach to information security. Departments and agencies should learn from the experiences of the QPS and be proactive in taking appropriate action, rather than waiting to become the subject of a similar inquiry in the future.

IMPLEMENTATION OF RECOMMENDATIONS

To discharge the CJC's statutory obligation to oversee the reform of the QPS, criminal law and the criminal-justice system, it will be important to follow-up on the implementation of the recommendations and consider how effective those recommendations have been in achieving the objectives of the report itself, and of the CJC more generally.

With regard to the recommendations affecting the QPS, the CJC favours the establishment of an implementation committee, with representation from the CJC, to oversee the implementation of recommendations of this report.

The two recommendations that were made regarding industry regulation for private investigators (chapter 8) become the responsibility of the Office of Fair Trading. There were also several recommendations made to government more generally (review of provisions for access to government information, privacy

legislation and the creation of a new offence to access confidential information).

The CJC will actively monitor the implementation of recommendations and prepare internal updates on a regular basis. A formal program of monitoring and evaluation will be established, with the goal of not only ensuring that recommendations have been implemented, but of assessing the effectiveness of the recommendations.

Given that this is a report pursuant to section 26 of the Act,³³ the CJC is currently intending to present a follow-up report to Parliament in the next two to three years. A two- to three-year time frame has been selected, as some of the recommendations made regarding the QPS will require funding and at least one complete financial planning cycle to budget and implement. This time frame is also suitable for those recommendations requiring legislative change.

The CJC will monitor and report on the implementation and effectiveness of the recommendations through a variety of publications; apart from the follow-up report itself, this may include the CJC Annual Report, reports to the PCJC, research and prevention reports and the QPS Monitor.

ENDNOTES

- [1] There are exceptions to this protection in s. 96(2) of the Act, which provides that such disclosures are admissible in proceedings for contempt of the CJC or for perjury.
- [2] The guidelines used by the Chairperson to make non-publication orders are outlined in appendix E.
- [3] Appendix F gives the names of the stakeholders who provided submissions and appeared at the Public Inquiry.
- [4] Reports considered in the preparation of this report but not specifically referenced are cited in the 'Further reading' list that follows the reference list at the end of this report.
- [5] 'A standard is a published document which sets out specifications and procedures designed to ensure that a material, product, method or service is fit for its purpose and consistently performs the way it was intended to.' (Standards Australia, **All about Standards**, downloaded from web site www.standards.com.au visited on 6.8.00).
- [6] Standards Australia is an independent company that prepares and publishes most of the voluntary technical and commercial standards in Australia. These standards are developed through an open process of consultation and consensus. Through a Memorandum of Understanding with the Commonwealth Government, Standards Australia is recognised as Australia's peak national standards body.
- [7] Examples of the types of information that should be classified as in-confidence are shown in appendix A.
- [8] See appendix G.
- [9] Section 23 of the Financial Management Standard 1997.
- [10] These standards are currently under review.
- [11] These officers were eliminated because they were able to demonstrate a legitimate police reason for accessing the information.
- [12] Lodged by the CJC officer who received the intelligence information about officers at the Nerang Police Station.
- [13] Source: CJC Complaints Database, as at 3 October 2000.
- [14] The structure of the ISS is shown in appendix J.
- [15] The structure of the IMD is shown in appendix K.
- [16] CITEC CONFIRM is described in detail on page 80–85.
- [17] Provisions in legislation, such as the PSAA, are discussed in chapter 9 ('Information Protection and the Law').
- [18] Mr Roger Clarke is currently a Visiting Fellow, Department of Computer Science, Australian National University, and Principal, Xamax Consultancy Pty Ltd. He has spent over 25 years in the IT industry and is well published in the area.
- [19] Now known as the Australian Council for Policing Research.
- [20] Mr O'Regan had read, and was in agreement with, the recommendation of the Office of NSW Ombudsman (1994) for the NSW Police Service to adopt a 'reason for transaction' requirement.
- [21] At that time Project Shield was a dedicated proactive multidisciplinary investigative team focusing on police corruption in relation to drugs.
- [22] Appendix T details ss. 67 and 68.
- [23] A court brief, or QP 9, is the document that the arresting police officer(s) provide to the police prosecutor; it details the police officer's (or officers') recollection of the events that led to the arrest.

[24] The **Corrective Services (Administration) Act 1988** has a secrecy provision (s. 61) that prohibits release of Corrective Services information unless it is for the purposes of a prescribed Act or the **Juvenile Justice Act 1992** or is required by a court or judge, or otherwise by law.

[25] For all offences, the court may make an order to vary the rehabilitation time.

[26] Quote from the letter sent to stakeholders with a copy of the draft Bill.

[27] At the time of writing.

[28] For present purposes, this licence will be referred to as a 'commercial agent's licence'.

[29] An officer is defined in the Security Providers Act as a director, secretary, executive officer or a person who can control or substantially influence the conduct of the corporation's affairs (s. 13).

[30] Some of the deficiencies were later corrected through amendments to the legislation.

[31] It should be noted that the ICAC report (1992a) recommended that industry regulation be the responsibility of the Department of Business and Consumer Affairs, New South Wales.

[32] A penalty unit may range from \$60 to \$100. Appendix W contains the meaning of a penalty unit under the **Penalties and Sentences Act 1992**.

[33] This section is described in chapter 1 ('Introduction').

APPENDIX A: EXAMPLES OF IN-CONFIDENCE MATERIAL

The following examples are taken from the NPRU report, A Standard Law Enforcement Information Security System: Guidelines for Law Enforcement Agencies (1995, pp. 29–30).

IN CONFIDENCE — Material for which this classification may be appropriate:

- Sensitive information concerning the private affairs of individuals, e.g.:
 - Personnel records.
 - Medical records.
 - Criminal history.
 - Accident report records.

- Information provided to the agency under an assurance or expectation of confidentiality, e.g.:
 - Complaints.
 - Allegations.
 - Personnel security vetting records.

- Information relating to criminal investigations, the premature release of which would inhibit the effectiveness of the agency.

- Routine reports and correspondence relating to operations requiring some short-term protection.

- Contractual and tender documentation.

- Routine audit reports.

- Sensitive industrial relations matters.

APPENDIX B: THE ICAC EXPERIENCE IN RELATION TO CONDUCTING PUBLIC HEARINGS

In deciding whether the CJC hearings on these matters should be open or closed, the NSW authority of *Chaffey v. Independent Commission Against Corruption* (1992) 30 NSWLR 21 provided some assistance. That case concerned a number of police officers who were the subject of an investigation by the ICAC. Evidence adverse to one of them, Chaffey, was to be given at public hearing of the ICAC. Chaffey objected to the evidence being given in public on the ground that in the circumstances of the case it would be unfair to do so. Chaffey was successful in the first instance but the decision was overturned on appeal to the NSW Court of Appeal.

The provision of the *Independent Commission Against Corruption Act 1988* ('the ICAC Act') which was being considered provided a wider discretion to the ICAC to hold hearings in public or private than the *Criminal Justice Act* does to the Commission.

Section 31 of the ICAC Act provides:

31. (1) A hearing may be held in public or in private, or partly in public and partly in private, as decided by the Commission.

...

(3) In reaching these decisions, the Commission is obliged to have regard to any matters which it considers to be related to the public interest.

In allowing the appeal the court (Kirby P, as he then was, dissenting) found that s. 31 confers an open discretion as to whether a hearing is held wholly or partly in private, subject to the requirement to consider matters related to the public interest and the overriding provisions of s. 12 to have regard to the protection of the public interest and the prevention of breaches of trust.

At page 30 Gleeson CJ (as he then was) said:

Considerations of public interest which support an open hearing, and which were taken into account by the Commissioner, include the need for public confidence in the operations of the Commission, and the assistance to the investigative process which might be gained from the giving of wide publicity to the allegations being investigated. It was for the Commission to determine the weight to be given to such considerations.

At page 30 His Honour referred to the Royal Commission on Tribunals of Inquiry under the Chairmanship of Lord Justice Salmon in 1966 who expressed the view that it is 'of the greatest importance that hearings before a Tribunal of Inquiry should be held in public. It is only when the public is present that the public will have complete confidence that everything possible has been done for the purpose of arriving at the truth'. After reading several passages of the report of the Salmon Commission, Gleeson CJ went on to observe at page 31:

A number of the matters referred to in these paragraphs are of relevance to the discretionary decision which the Commission had to make in the present case, and tend to support (the decision to hold hearings in public). What is of particular interest for present purposes is that the process of reasoning set out above involves a conscious weighing of the public interest in openness of

proceedings against the harm to reputation that can result. It is the same process as is required by s 31 of the Independent Commission Against Corruption Act and as was undertaken by the Commission in the present case.

It is, of course, true that the Salmon Report stressed that Royal Commissions are rare occurrences. The Independent Commission Against Corruption is sometimes referred to in popular discussion as a kind of standing Royal Commission. It may be doubted that people who see it in that light understand how relatively infrequently Royal Commissions have been held in the past, or why that is so. One reason relates to their propensity to infringe civil liberties and cause extensive damage to reputations. Nevertheless, when Parliament established the Commission, with its inquisitorial procedures, and its capacity to over-ride basic common law rights, it must have appreciated the potential for damage to the reputations even of innocent people that was involved.

Even though the ICAC legislation differs significantly to the Act these observations are relevant here. In particular, the view that considerations of public interest include the need for public confidence in the operations of the CJC and the assistance to the investigative process which might be gained from giving wide publicity to the allegations being investigated.

In the second of the majority judgments Mahoney JA stated at pages 60–61:

Where a proceeding is to be heard in public, a party to it may well suffer harm from the publicity of it. That harm may range from mere embarrassment to grave damage to reputation. However, the fact that will result if the discretion be exercised in favour of a public hearing does not mean that the party has not been dealt with with procedural fairness. In some cases, the public interest or other ends to be served by the discretion may outweigh the right of the individual not to be harmed by the proceeding. In so far as legitimate expectation or the like is relevant, parties involved in such proceedings may not expect that in no circumstances may their reputation suffer from their involvement.

I do not mean by this that the fact that harm may be done to an individual by a public hearing is to be treated lightly in the exercise of such a discretion. Publicity is not an end in itself. It is the means by which, as experience has shown, more fundamental purposes are to be served. The proper scrutiny of the exercise of power and the creation of confidence in those who exercise it are involved. But, in the end, the result which is sought by procedural fairness and the other rules of law is that every individual be treated justly under the law.

APPENDIX C: LEGAL ADVICE ON CONDUCTING A PUBLIC HEARING

Prior to the CJC hearing, advice was obtained from Mr R A Mulholland QC, as to whether the circumstances of this matter would permit a public hearing pursuant to the provisions of the Act.

Mr Mulholland opined:

By the substitution of ‘closed’ for ‘open’ in s. 90 of the Act, Parliament is to be taken to have decided that, in the ordinary case, the prospect of damage to an individual’s reputation will outweigh public interest factors which support an open hearing. In other words, the Act now implies that the public interest favours a closed hearing ... Furthermore, the discretion to order a public hearing is conditional on the Commission considering that a closed hearing would be unfair to a person or contrary to the public interest and this assessment must have regard to the subject matter of the hearing and the nature of the evidence expected to be given: s. 90(2) of the Act. The barrier is therefore set high before a public hearing will be justified.

It is necessary to approach the question relating to the form of hearing without preconceived notions that a public hearing will enhance public confidence in the integrity of the Commission’s operations and thus serve the fundamental purposes for which it was established. In my view, before ordering a public hearing, the Commission must form a definite view that, having regard to the facts and circumstances connected to the subject matter of the hearing and the nature of the evidence anticipated to be given, a closed hearing would be unfair to a person or contrary to the public interest. Of particular relevance in this case is the need to show that a closed hearing would be “contrary to the public interest”. This does not mean that the matters which, according to the orthodox view, are telling in support of a public hearing should be ignored. But it does require that, before a public hearing can be ordered, the Commission will have to be satisfied that the reasons for a public hearing outweigh those against to the extent that a closed hearing would be contrary to the public interest.

The factors which may be said to be in favour of a public hearing in the current investigation are as follows:

- The unauthorised disclosure of confidential information by police is a serious issue which has not been properly or adequately addressed by the QPS;
- Evidence has been uncovered of widespread misuse of the QPS database for unofficial purposes by police officers and others;
- Despite extensive investigation (including closed hearings) unearthing a substantial amount of evidence, there is good reason to suspect that many officers have lied during the course of disciplinary interviews and this is constituting a serious impediment to the progress of the investigation;
- The Commission believes that public, as opposed to private, hearings provide the most effective method of advancing the current investigation because public examination is more likely to encourage witnesses (specifically the QPS officers who have so far lied) to tell the truth, generate public information and submissions germane to the investigation and, ultimately, provide the best opportunity for ascertaining the truth and helping to eliminate or reduce unauthorised disclosures by police.

Whilst the above are factors for the Commission to weigh and consider, in my view taken as a whole the circumstances are sufficient to warrant a conclusion that to rely exclusively on closed hearings would be contrary to the public interest. It follows from what I have said that I do not regard it as a necessary pre-requisite for public hearing that the investigation will 'fail' without them. However, I repeat my view that the Commission should approach its determination conscious of the legislative intention that extends paramountcy to the protection of an individual's reputation.

APPENDIX D: ANNOUNCEMENT OF CJC INQUIRY

CRIMINAL JUSTICE COMMISSION • NOTICE OF PUBLIC HEARING

Pursuant to its responsibility under the **Criminal Justice Act 1989** to investigate alleged or suspected misconduct or official misconduct in the Queensland Police Service (QPS) the Criminal Justice Commission (CJC) is currently investigating whether members of the QPS have obtained unauthorised access to, and/or make unauthorised disclosure of, confidential information held by the QPS principally on its computer data base.

The CJC is also investigating and developing measures for preventing and detecting misconduct of this kind.

For the purposes of the investigation the CJC has resolved to conduct public hearings commencing on 14 February 2000 at the offices of the CJC, 557 Coronation Drive Toowong. The Chairperson, Mr Brendan Butler SC, will conduct the hearing.

The CJC has also directed that a report of the said investigation and hearings be furnished to the Commission with a view to the Commission making a public report.

Any person interested in making a submission, or providing information, to the CJC on this issue and/or appearing before it at the public hearing is invited to contact the Commission by writing to:

PO Box 137
Brisbane Albert Street Qld 4002

Or

www.cjc.qld.gov.au.

or

mailbox@cjcc

Submissions to appear before the CJC should be received at the CJC by no later than 5pm on 10 February 2000

APPENDIX E: GUIDELINES USED TO MAKE NON-PUBLICATION ORDERS DURING THE PUBLIC HEARING

The CJC Chairperson was careful to formulate guidelines as to the manner in which he would exercise the Commission's discretion to prohibit the publication of identifying particulars of individuals appearing before the Public Inquiry. In this regard he concluded that where a person admitted his or her involvement in unlawful activity or misconduct or where there was a significant body of evidence against that person then generally disclosure of the person's identity was not considered unfair to the person. The extent and seriousness of the alleged unlawful behaviour or misconduct was also a factor in the exercise of that discretion.

On the other hand, if an assertion was made in evidence by a witness that another person had engaged in unlawful activity but the assertion was totally unsupported, or was made gratuitously, and no attempt was made to support the assertion then ordinarily publication of the person's name would have been unfair. Of course there were often cases in between and the discretion needed to be considered in respect of each individual who appeared before the Commission in respect of whom there was adverse evidence. These considerations only applied to those who were present at the hearings and who were able to comment on the evidence against them. Publication of the names of those who were not required to appear was prohibited.

APPENDIX F: LIST OF STAKEHOLDERS WHO MADE SUBMISSIONS TO THE INQUIRY

NAME	ORGANISATION	DATE OF APPEARANCE	WRITTEN SUBMISSION RECEIVED
Dr D J Brereton	CJC	06 March 2000	✓
Mr C Strofield, Mr D Luttrell, Superintendent I Stewart and Inspector R Gee	QPS	06 March 2000	✓
Mr J Just	QPS	06 March 2000	✓
Mr A Skippington and Ms R Cunningham	CITEC CONFIRM	06 March 2000	✓
Commander P Cornish	South Australia Police	06 March 2000	✓
Chief Superintendent K Rynders	QPS	06 March 2000	✓
Mr S J Kinmond	New South Wales Deputy Ombudsman	06 March 2000	✓
Chief Superintendent C Crawford	ESC QPS	07 March 2000	✓
Commander M J Brammer	Special Crime and Internal Affairs, New South Wales Police Service	07 March 2000	✓
Mr G C Taylor	Australian Privacy Charter Council	07 March 2000	✓
Supt. J Ashby	Victoria Police Service	07 March 2000	✓
Mr P J G Laurens	Institute of Mercantile Agents	07 March 2000	✓
Mr S Reidy	Queensland Law Society	07 March 2000	✓
Mr I F M Dearden	President, Queensland Council for Civil Liberties	08 March 2000	✗
Mr G Wilkinson, Mr D Sycz and Mr G Cranney	Queensland Police Union of Employees	08 March 2000	✓
Ms C L Allinson	Information Security Section, Queensland Police Service	08 March 2000	✓

NAME	ORGANISATION	DATE OF APPEARANCE	WRITTEN SUBMISSION RECEIVED
Professor W J Caelli	Head of School, Data Communications, QUT	08 March 2000	✓
Mr A J H Morris QC and Mr C J Strofield	QPS	08 March 2000	✓
Mr B Chapman	Director, SCEID Consultancy Services Pty Ltd	Did not appear	✓
Mr G Walters	Manager, Fraud Prevention, Internal Assurance Branch, Australian Tax Office	Did not appear	✓

APPENDIX G: INFORMATION PRIVACY PRINCIPLES (AUSTRALIAN COMMONWEALTH)

The Information Privacy Principles are as follows:

Principle 1 — Manner and purpose of collection of personal information

1. Personal Information shall not be collected for inclusion in a record or in a generally available publication unless:

- (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collection; and
- (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2 — Solicitation of personal information from individual concerned

Where:

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of.

- (c) the purpose for which the information is being collected;
- (d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and
- e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or anybody or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3 — Solicitation of personal information generally

Where:

- (a) a collector collects personal information for inclusion in a record or in a record or in a generally available publication; and
- (b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

- (c) the information collected is relevant to that purpose and is up to date and complete; and

- (d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4 — Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

- (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5 — Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

- (a) whether the record-keeper has possession or control of any records that contain personal information and;
- (b) if the record-keeper has possession or control of a record that contains such information;
 - (i) the nature of that information;
 - (ii) the main purpose for which that information is used; and
 - (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

- (a) the nature of the records of personal information kept by or on behalf of the record-keeper;
- (b) the purpose for which each type of record is kept;
- (c) the classes of individuals about whom records are kept;
- (d) the period for which each type of record is kept;
- (e) the persons who are entitled to have access to personal information, contained in the records and the conditions under which they are entitled to have that access; and
- (f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

- (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
- (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6 — Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7 — Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

- (a) is accurate; and
- (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

- (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
- (b) no decision or recommendation to the effect that the record, should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8 — Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9 — Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10 — Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

- (a) the individual concerned has consented to use of the information for that other purpose;
- (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
- (c) use of the information for that other purpose is required or authorised by or under law;
- (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record keeper shall include in the record containing that information a note of that use.

Principle 11 — Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

- (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
- (b) the individual concerned has consented to the disclosure;
- (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of the individual concerned or of another person;
- (d) the disclosure is required or authorised by or under law; or
- (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

APPENDIX H: EXCERPT FROM THE QUEENSLAND GOVERNMENT INFORMATION STANDARD 24 (PRIVACY AND CONFIDENTIALITY)

Principle 7 Privacy and Confidentiality

Each agency should ensure the privacy and confidentiality of its information resource, and take all reasonable precautions to ensure that personal information (about individuals), commercial-in-confidence information (about organisations), or other sensitive information is not misused, intentionally or unintentionally, either within the agency or when shared with external organisations.

The Queensland Government will be reviewing its position with regard to Information Privacy in the near future. However, each agency should be aware of the Information Privacy Principles contained in the Commonwealth Privacy Act 1988 (Refer to World Wide Web site http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html), and use them as guidelines where appropriate in the development of agency privacy policies. Note, however, that these are currently not binding on Queensland Government Agencies. The Commonwealth recently developed the National Principles for the Fair Handling of Personal Information which are intended to set a benchmark for all organisations which handle personal information regardless of the industry sector, jurisdiction, or field of activity (refer http://www.privacy.gov.au/news/p6_4_1.html).


Agencies may need to reassess the collection and use of information, to ensure that only required data is collected. This is particularly relevant where there are privacy or confidentiality considerations. Both legislative and agency requirements change, and in many cases, information is collected because 'it has always been collected', even though the business of the agency may have changed over time.

To meet the requirement for privacy and confidentiality, each agency should develop and implement appropriate policies and practices to ensure that information or data which is deemed to be 'private' is made accessible only to those who are authorised. When developing and documenting privacy policies, sensible consideration should also be given to the Freedom of Information Act 1992 (Qld).

Each agency is accountable for the release of information within its care, and should have policies and practices in place regarding the release of that information. These should take into consideration freedom of information and privacy issues. Where confidentiality of private sector information is an issue, agencies should consider using mechanisms such as confidentiality agreements to protect both parties.

(Source: Queensland Government web site visited in April 2000)

APPENDIX I: THE QPS SELF TEST



Would Your Decision Pass The Test?

Consider

Would your decision withstand **Scrutiny?**

- Community
- Police Service
- Media

Will your decision **Ensure compliance?**

- Oath of Service
- Policy
- Code of Conduct

Is your decision **Lawful?**

- Laws
- Regulations
- Rules

Is your decision **Fair?**

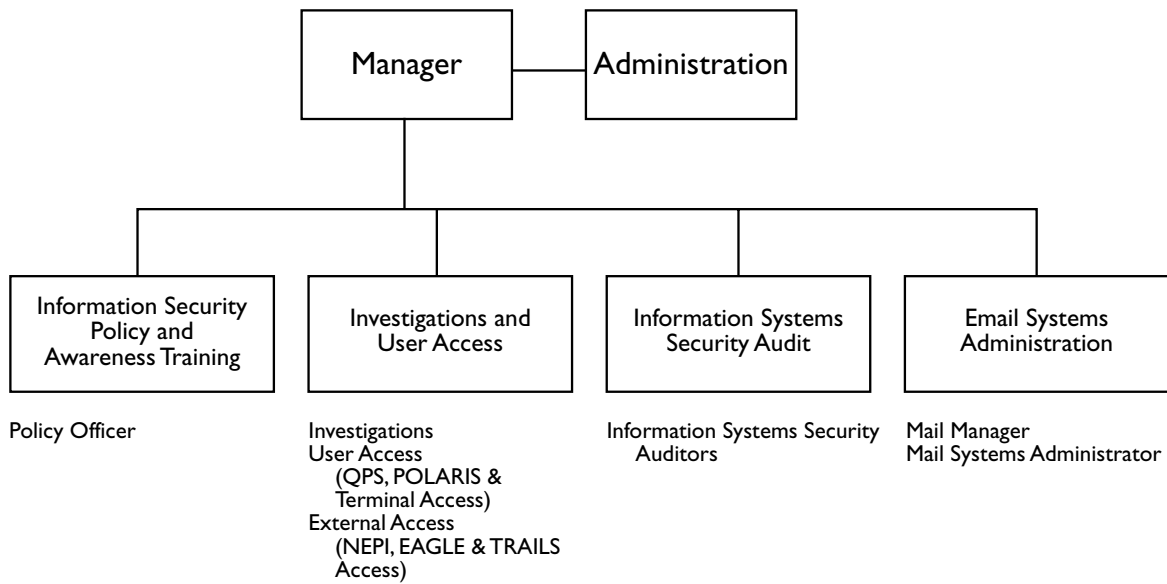
- Community
- Colleagues
- Your Family
- Others

before you decide.

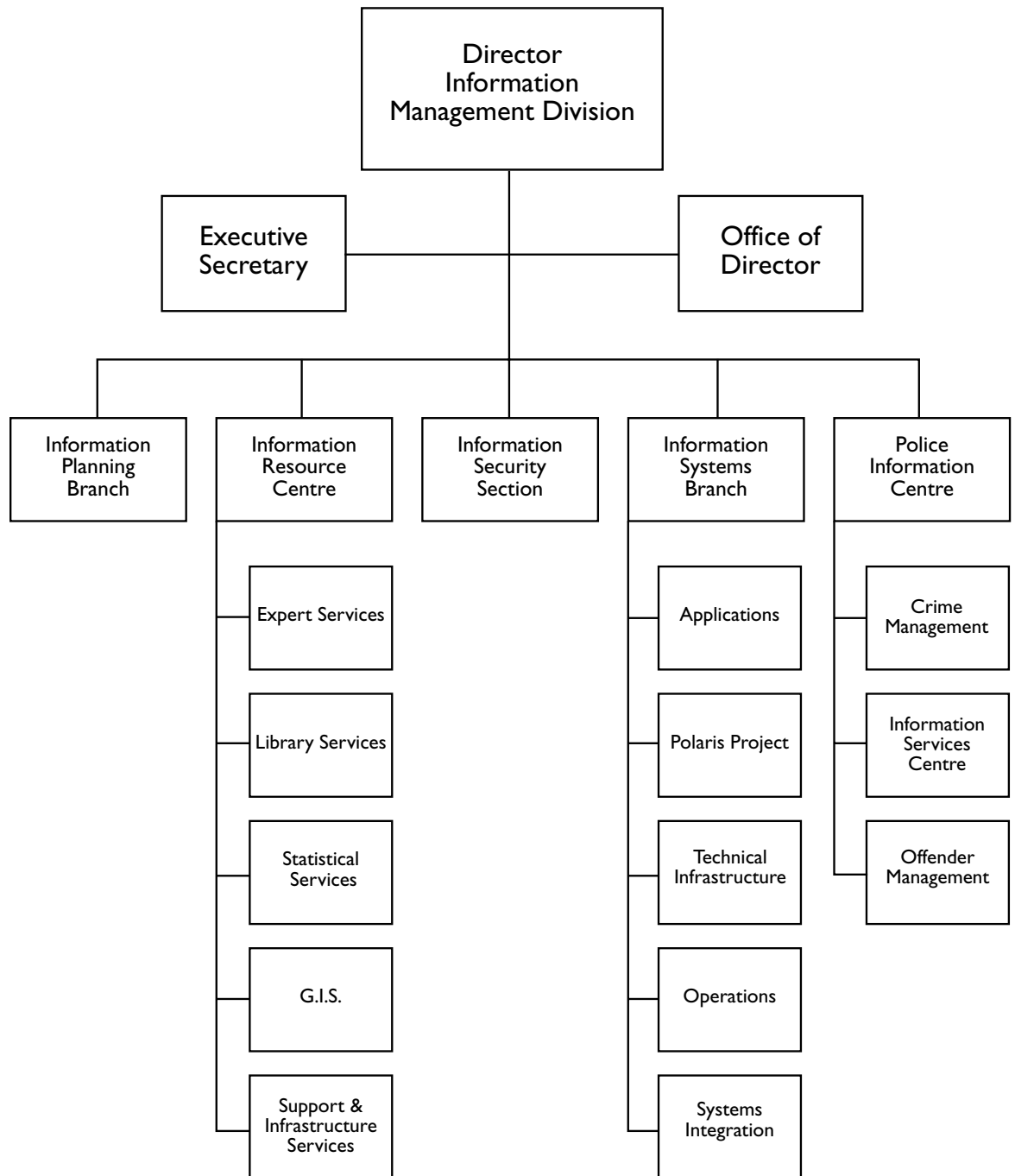
An unethical decision will affect us all

(Produced by The Ethical Practice Branch, Ethical Standards Command.)

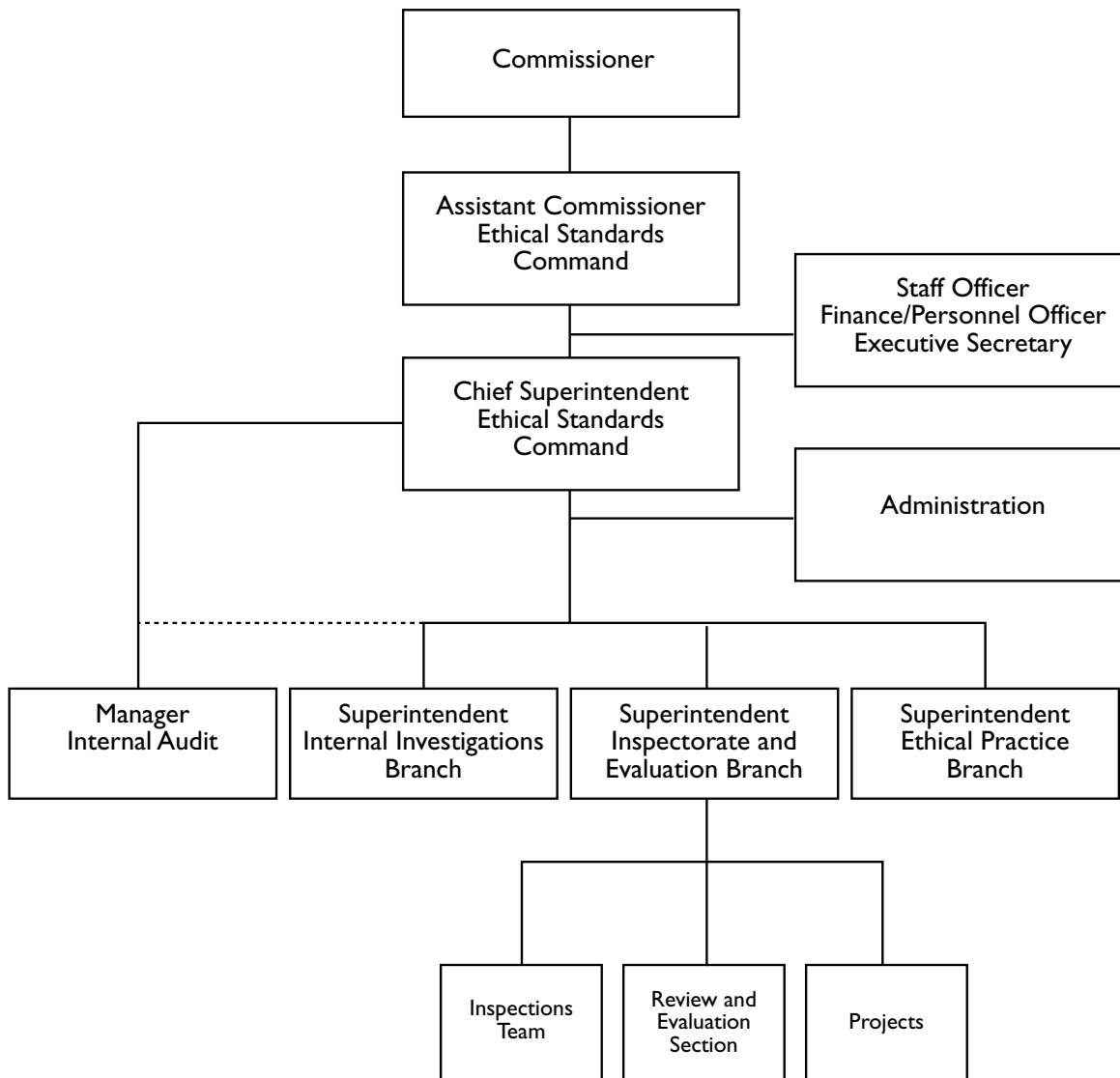
APPENDIX J: STRUCTURE OF THE INFORMATION SECURITY SECTION, QPS



APPENDIX K: STRUCTURE AND REPORTING RELATIONSHIPS OF THE INFORMATION MANAGEMENT DIVISION, QPS



APPENDIX L: STRUCTURE AND REPORTING RELATIONSHIPS OF THE ETHICAL STANDARDS COMMAND, QPS



APPENDIX M: QPS ASSESSMENT CRITERIA FOR OUTSIDE EMPLOYMENT

Assistant Commissioners, Directors and Executive Managers are to assess the appropriateness of outside employment using the following criteria:

- the potential for conflict with the member's responsibilities (this criterion is particularly relevant to officers and police recruits especially where the outside employment is in industries such as security, education/training, transport or liquor related industries);
- the potential for the Service to be legally liable as a result of the member undertaking such employment;
- the hours of work required in the outside employment and the likelihood of those hours adversely affecting the member's ability to fulfil normal duties;
- the level of risk of injury to the member in the course of the outside employment;
- the likelihood of the Service being liable for any injury to the member or a member of the public as a result of the proposed outside employment;
- the public reputation of the company or establishment and the nature of the business where the member seeks employment; and
- any other relevant factors.

The major considerations in any assessment process for outside employment shall be the preservation of the integrity of the Service and the avoidance of any actual or apparent conflict of interests.

Assistant Commissioners, Directors or Executive Managers are to monitor outside employment undertaken by members under their control and prohibit any such outside employment which is considered inappropriate, or in breach of the provisions of s. 10.9 of the Code of Conduct.

Any written advice received from members on outside employment in the security, transport or liquor related industries are to be forwarded to the Executive Director, Operations with an appropriate recommendation by the relevant Assistant Commissioner, Director or Executive Manager for consideration.

Source: HRMM s.17.2 under 4.5.3

APPENDIX N: LOG-IN WARNING SCREEN FOR POLARIS

QUEENSLAND POLICE SERVICE

WARNING - CONDITIONS OF ACCESS TO AND USE OF THIS COMPUTER SYSTEM

1. Access to and use of any information on this computer system is for authorised users only. Any Unauthorised access and use, eg the use of another's User-ID and Password, is strictly prohibited. By accessing or using this system you are representing that you are an authorised user. You are NOT authorised to access information for personal reasons.
2. The information contained on this computer system is confidential and must not be disclosed to unauthorised persons. Improper disclosure of information is an offence against section 10.1 of the Police Service Administration Act 1990.
3. Making unauthorised copies of software is a criminal act and can expose you to punishment or civil claims. Use only authorised software.
4. Details of all transactions, including User-IDs, are automatically recorded by the computer and can be retrieved. By accessing and using this computer system you are consenting to security monitoring.
5. Malicious entry of false information is strictly prohibited. Any member who maliciously enters false information may be liable to be dealt with for misconduct.

User Id: _____
Password: _____

Continue (Pause) Exit (F12) Help (Insert)

APPENDIX O: LOG-IN SCREEN FOR THE QPS SYSTEM

```
|||      ||      ||      ||      ||      ||      ||      ]
          QQQQQQ      PPPPPPPP      SSSSSSS
          QQ      QQ      PPP      PPP      SSS      SSS
          QQ      QQ      PPP      PPP      SSS
          QQ      QQ      PPPPPPPPP      SSSSSSS
          QQ      QQ      PPP      SSS      SSS
          QQ      QQ      PPP      SSSSSSS
          QQQQQQ      PPP
          QQQ
          ** WARNING **
*****
* This system's information is confidential and must not be disclosed to un- *
* authorised persons. Section 10.1 of the Police Service Administration Act *
* provides a penalty for improper disclosure of information. *
* Details of all transactions, including User-IDs, are automatically recorded *
* by the computer and can be retrieved. Use of the computer system constitutes *
* consent to security monitoring. *
* In your own interest, do not permit anyone to use your User-ID and password, *
* always log out of each system at the completion of any terminal inquiry and *
```

APPENDIX P: EXCERPT FROM POLICE AND DRUGS: A FOLLOW-UP REPORT (1999A)

The following excerpt is taken from Police and Drugs: A Follow-up Report (1999, p. 33–34) and outlines the CJC’s comment on the decision of the QPS to not introduce a ‘reason for transaction’ field.

It is the view of the CJC that the QPS should continually endeavour to improve and implement risk management tools. It is fair to say that the adoption of any ‘security’ practices will always incur financial costs and present some inconvenience to the workers affected; in this case, staff will be required to perform an additional action when conducting checks on databases. However, the decision as to whether this particular risk management tool should be adopted needs to be based on a broader array of factors, such as:

Potential for misuse of databases — As Project Shield revealed, the accessing of databases for inappropriate and unlawful purposes was extremely common. Not only can police officers access a database directly, they are easily able to direct or request another person to do so on their behalf. In either case there is no requirement to record the identity of the inquirer (only the individual logged onto the system when the inquiry is made) or the reason the inquiry is being made.

Given the lack of quantitative evidence from which to generalise, it is impossible to estimate the full extent of the inappropriate and unlawful accessing of databases, but based on what is known through complaints and the Police and Drugs Inquiry, there is evidence that misuse of confidential information continues to be a problem. Each year, the CJC’s complaints database records a number of cases that raise suspicion of improper access by police officers to confidential information. In the last financial year (1997–98), the CJC received 117 allegations of police disclosing or passing on confidential information (involving approximately 77 police officers). The motivation for improper access may range from misplaced helpfulness/loyalty to financial gain or other improper purposes. Whatever the motive, the disclosure has the potential to compromise an investigation and the safety of officers, especially undercover operatives and cooperating witnesses.

Effectiveness of current accountability mechanism — As was found during Project Shield, it was often impossible to verify the reasons for many of the enquiries made.

Financial cost of proposed accountability mechanism — The cost of compliance can be minimised by design features such as pull-down menus and/or standard identification codes (e.g. codes for different types of reasons). However, it is accepted that the integration of a field would present some cost to the QPS. It is understood through correspondence with the QPS that earlier versions of POLARIS had a ‘reason for transaction’ field built-in, but that this facility was not further developed in later versions.

Cost benefits of proposed accountability mechanism — Wherever the potential for misuse is reduced there are cost benefits through savings on investigations etc. Some additional hidden saving will result as police officers and staff cease performing unnecessary enquiries.

It has been argued that police who are intent on making unauthorised releases of

information would manufacture a plausible reason to accommodate the requirements of the system. Clearly, no system can guarantee that abuses of this kind will not occur; however, imposing a requirement to record reasons for access would be an improvement on having no deterrent at all and would help ensure that officers requesting another person to conduct an inquiry on their behalf (e.g. officer or civilian) are identified and questioned as to their reason for access.

APPENDIX Q: DOCUMENTS AND REPORTS AVAILABLE FROM TIRS AND CRISP

TIRS — The following documents may be ordered from CITEC CONFIRM by authorised users online for counter pick-up or postal delivery:

- Breach results
- Police breach report
- PT51 diagram
- TAIS report
- TAIS sketch plan
- Signed Statements
- QPS Mechanical Inspection Report
- QT Mechanical Inspection Report
- Other authorised mechanical inspection reports

TIRS — The following documents are available from CITEC CONFIRM to authorised users upon finalisation of coroners' inquiries with the exception of those required for a coronial inquest.

- Police report to Coroner
- Coroner's Report
- Post mortem certificate
- Autopsy report
- Specimen results report
- Life extinct form
- Medical Practitioner's Certificate
- Property Inventory (QP35)
- Reports from driver, victims, witnesses
- Doctor's record
- Ambulance Report
- Police Court Brief

CRISP — The following reports or documents are available from CITEC CONFIRM to authorised users online for counter pickup or postal delivery:

Summary of crime details

- crime number
- date, time and reporting station
- major crime
- address of offence
- date of offence
- crime status

Complainant details

- name
- address (street and suburb)

Informant/Witness details

- name
- address

Property details

- make, model, description, serial number and any inscription
- value, lien amount and subrogation rights
- claim number

Modus Operandi

- details of what the offender did
- point of entry into the premises
- how entry was gained
- whether damage was caused
- reference to property taken
- other points of interest about the offence
- how the offender left the premises

Other crime classes

- additional crimes committed

Recovery details

Details of recovered property including recovery location

Source: <http://www.citec.qld.gov.au/confirm.html>

APPENDIX R: REASON FOR TRANSACTION FIELD IN THE TIRS AND CRISP SYSTEMS

TIRS - Traffic Incident Reporting System
Reason For Access

Please enter Claim/File Number or reason for accessing this report. Also indicate if you are representing another person or organisation.

Claim/File Number: []

Reason: []

Representing: []

Note: The reason for transaction field for CRISP is identical to the above shown for CRISP.

APPENDIX S: CITEC CONFIRM FEES FOR SEARCHES ON VEHICLE REGISTRATIONS, TIRS AND CRISP DATABASES

Vehicle Registrations (owned by Queensland Transport)

Enquiry (using registration number) – Current	\$10.00
Enquiry (using registration number) – Point-In-Time	\$10.00
Alpha Search	\$16.00
Bulk Search	\$ 6.00
Declaration	\$16.00

Traffic Incident Reports (owned by QPS)

Police Report	\$56.10
Revisit Police Report (within 60 days)	\$ 6.60
Police Report Plus Other Documents	\$67.10
Other Documents	\$17.60
Enforcement Action Only	\$17.60
Renew Lapsed Order	\$16.00

Crime Reports (owned by QPS)

Crime Report	\$56.10
Crime Report Follow-Up	\$ 7.70
List of Updated Crimes	\$26.40
Add Subrogation / Property Details	\$ 0.00
Subrogation / Property Report	\$ 0.00

Source: CITEC CONFIRM and the Police Information Centre, QPS (July 2000)

APPENDIX T: SECTIONS 67 AND 68 OF THE TRANSPORT OPERATIONS (ROAD USE MANAGEMENT VEHICLE REGISTRATION) REGULATION 1999

Division 5 of this Act is entitled 'Release of information'. Section 67 provides definitions. Section 68 is concerned with release of information on payment of fee.

67. In this division —

"client user", of a public access provider, means an eligible person who has —

- (a) entered into a public access agreement with the public access provider; and
- (b) been granted approval by the chief executive to be given details about a particular vehicle, as at a stated date, from the register.

"eligible person" means —

- (a) an involved person; or
- (b) a local agency; or
- (c) the registered owner of a vehicle seeking information from the register about the vehicle; or
- (d) a safety recall agency; or
- (e) a statutory authority.

"involved person" means a person who proposes to commence, or has commenced, litigation.

"litigation" means a proceeding, or a proposed proceeding, in a court for which information in the register about a particular vehicle is, or may be, of relevance, including, for example, a proceeding —

- (a) about a vehicle crash on a road or somewhere else; or
- (b) about the bankruptcy or possible bankruptcy of the registered owner of a vehicle; or
- (c) about fraudulent activities of the registered owner of a vehicle; or
- (d) that is before the Family Court of Australia and involves the registered owner of a vehicle.

"local agency" means a statutory body enforcing a law about the parking of vehicles in an area under its control.

"public access provider" means a person who has entered into an agreement with the chief executive to provide on-line computer access to the register to eligible persons.

"safety recall agency" means a vehicle manufacturer conducting a national vehicle safety recall program who requires details from the register to identify the registered owners of particular vehicles.

“statutory authority” means —

- (a) a statutory body, other than a local agency, enforcing laws about vehicles; or
- (b) a person that has lawful access to details kept by the chief executive in the register.

68.(1) The chief executive may give an extract from the register of information about a vehicle to an eligible person, or a person acting on the eligible person’s behalf, if the eligible person, or the person acting on the eligible person’s behalf

-
- (a) submits a request for the information to the chief executive in the approved form; and
 - (b) pays the relevant fee.
- (2) A public access provider may give an extract from the register of information about a vehicle to a client user of the public access provider on payment of the relevant fee.

APPENDIX U: EXCERPT FROM ICAC REPORT ON THE UNAUTHORISED RELEASE OF GOVERNMENT INFORMATION (1992)

The following excerpt details the recommendations made with regard to industry regulation for private investigator and commercial agents in New South Wales (pp. 130–33).

RECOMMENDATIONS

Measures should be taken as a matter of urgency to ensure more effective control. At present at least, that must come from outside the industry. Direction, supervision and careful monitoring are essential.

The following steps are recommended:

1. Abolish the distinction between commercial agents and private inquiry agents.
2. Retain the requirement that they be licensed.
3. Place control of the industry and responsibility for administration of the relevant legislation in the hands of the Department of Business and Consumer Affairs.
4. Revise licensing provisions, to control or prevent circumvention of the licence requirement by either unlicensed employers or the use of unlicensed employees. A general revision of the exemptions is required.
5. Specify qualifications required for the grant of a licence, having regard to the TAFE course. Consider similar qualification for applicants for first time sub-agents' licences. Consider whether persons simultaneously engaged in other occupations, e.g. police, should be ineligible.
6. Revise licensing procedures, so as to require:
 - (a) character references from suitably qualified persons, certifying the applicant to be of good fame and character and a fit and proper person to hold a licence;
 - (b) advertisement of all applications;
 - (c) proper procedures for objections and hearings.
7. Create a code of conduct, and require adherence to it, with suspension of licence and disqualification of licensee among sanctions for breach.
8. Code of conduct to include prohibition on:
 - (a) handling proscribed forms of information;
 - (b) proscribed methods of obtaining information.
9. Provide for regular and spot checks on accounts and records of licensees, as part of the supervisory role of the Department of Business and Consumer Affairs; that power to be exercised by officers of the Department, police or other duly authorised persons.
10. Establish and pursue a policy of stricter enforcement of statutory requirements.

Comment on recommendations

Management of the private investigation industry is a subject worthy of a lengthy report on its own. However, so much is to be covered in this Report, that it is not possible to present these recommendations in more than note form. Some brief comment on them is appropriate.

Recommendation No. 1

The present distinction between the two classes of agent is blurred. Uncertainty has many taking out both licences. The functions of both types of agent, are likely to include seeking to locate people. Both have been heavily involved in the illicit trade in confidential government information. In that respect, the same controls are needed for both. If there are to be some persons licensed for limited purposes only, that could be achieved by having separate classes of licence, as is done with drivers of motor vehicles. However, in most professions and trades, there is a basic qualification and a single licence or practising certificate, even for those who specialise.

Recommendation No. 2

Licensing is necessary both to limit participation to those who are suitable, and to control and supervise the industry. Control and supervision are necessary, because the conduct of both types of agent directly impinges on the rights of citizens. It is not simply a matter of seeking to regulate the relationship between agent and client; most clients of commercial and private inquiry agents can probably look after their own interests. It is the person who is the subject of the investigation or other proceeding – the person whose privacy may be invaded, or who may be harassed – in whose interests protection is required.

Recommendation No. 3

Both the Department of Business and Consumer Affairs, and the Police Service, will have an interest in the conduct of the agents' business. Involvement of the Department is appropriate to place the industry on a proper footing, and should improve both its quality and its acceptance as a legitimate business activity. Department officers should have a great deal to contribute to the industry's efficiency, standards and reputation. Involvement of the Police should not include management of a registry, or of the industry generally. It should be limited to their proper role of investigation, and crime prevention and detection.

Recommendation No. 4

Unlicensed persons have been doing much of the work of commercial and private inquiry agents, both within and outside the law. Mr Bartley identified some of the former; Mr Rindfleish ... was an example of the latter. The Act should be looked at, with a view to minimising the former; the latter is a matter for enforcement measures (see Recommendation 10).

Recommendation No. 5

Qualifications, and the special position of serving and former police officers, have been considered earlier in this chapter.

Recommendation No. 6

If there is to be provision for objections, there should be provision for advertisement. The special nature of the industry suggests that an objection procedure will remain appropriate, even when control of the industry passes to the Department of Business and Consumer Affairs. The right to object ought not to be limited to the Police.

Recommendations Nos. 7–8

A code of conduct, linked with licensing, puts the licensee's livelihood in jeopardy if he or she steps outside the code. In an industry in which many are known to have flouted common standards of probity and integrity, that is clearly needed. The code should form part of the agents' TAFE course, and instruction in it should be required of current licence holders.

Recommendations Nos. 9–10

These enforcement measures are necessary to the success of the controls proposed.

Conclusion

The industry may be able to contribute to the program of management proposed, but that could not be achieved at this time through the existing industry associations. They are too steeped in the old culture. As with all industries, the goal should be maximum participation by the industry itself and by consumer groups. But this industry at this time, by reason of its nature and its recent history, needs external control. The fitness of many who presently engage in it, should be reviewed.

APPENDIX V: SCHEDULE OF OFFENCES UNDER THE CRIMINAL CODE EXCLUDING APPLICANTS FROM OBTAINING A PRIVATE INVESTIGATOR LICENCE

PART 1 – EXISTING PROVISIONS

- Chapter 9 (Unlawful assemblies – breaches of the peace)
- Chapter 16 (Offences relating to the administration of justice)
- Chapter 20 (Miscellaneous offences against public authority)
- Chapter 28 (Homicide – Suicide – Concealment of birth)
- Chapter 29 (Offences endangering life or health)
- Chapter 30 (Assaults)
- Chapter 32 (Assaults on females – Abduction)
- Chapter 33 (Offences against liberty)
- Chapter 36 (Stealing)
- Chapter 37 (Offences analogous to stealing)
- Chapter 38 (Offences with violence – Extortion by threats)
- Chapter 39 (Burglary – Housebreaking and like offences)
- Chapter 40 (Other fraudulent practices)
- Chapter 41 (Receiving stolen or fraudulently obtained and like offences)
- Chapter 42 (Frauds by trustees and officers of companies and corporations – false accounting)
- Chapter 42A (Secret commissions)
- Chapter 46 (Offences)
- Chapter 49 (Punishment of forgery and like offences)
- Chapter 52 (Personation)
- Chapter 56 (Conspiracy)

PART 2 – PROVISIONS REPEALED BY CRIMINAL LAW AMENDMENT ACT 1997

- Section 343A (Assaults occasioning bodily harm)
- Section 344 (Aggravated assaults)

APPENDIX W: MEANING OF PENALTY UNIT UNDER THE PENALTIES AND SENTENCES ACT 1992

5.(1) The value of a penalty unit is —

- (a) for the **Justices Act 1886**, part 4A, or an infringement notice penalty under the part — \$60; or
- (aa) for the **Cooperatives Act 1997** — \$100; or
- (b) in any other case, for this or another Act — \$75.

(2) If an Act expresses a penalty or other matter as a number (whether whole or fractional) of penalty units, the monetary value of the penalty or other matter is the number of dollars obtained by multiplying the value of a penalty unit by the number of penalty units.

(3) If an order of a court expresses a penalty or other matter as a monetary value, the number of penalty units is to be calculated by dividing the monetary value by the value of a penalty unit as at the time the order is made.

(4) For the purposes of this or another Act a reference to a penalty of a specified number of penalty units is a reference to a fine of that number of penalty units.

Example:

‘Maximum penalty — 10 penalty units’ means the offender is liable to a maximum fine of 10 penalty units.

REFERENCES

- Akindemowo, O. 1999, *Information Technology Law in Australia*, LBC Information Services, Sydney.
- Australian Law Reform Commission 1983, *Privacy*, Canberra.
- Chan, J., Brereton, D., Legosz, M. & Doran, S. (forthcoming), *The Impact of Information Technology on Policing: An Australian case study*. [Final report to be submitted to the Criminal Justice Commission and the Australian Research Council.]
- Criminal Justice Commission 1997a, *Police and Drugs: A Report of an Investigation of Cases involving Queensland Police Officers*, CJC, Brisbane.
- 1997b, *Integrity in the Queensland Police Service: Implementation and Impact of the Fitzgerald Inquiry Reforms*, CJC, Brisbane.
- 1999a, *Police and Drugs: A Follow-up Report*, CJC, Brisbane.
- 1999b, *Ethics Surveys of First Year Constables: Summary of findings 1995–1998*, CJC, Brisbane.
- 2000, *Public Attitudes towards the Queensland Police Service*, CJC, Brisbane.
- unpub., *Transcripts of the Public Inquiry into the Alleged Unauthorised Access and/or Release of Confidential Information from Police Computers by Members of the Queensland Police Service (14 February 2000 – 1 March 2000) (Mr B. J. Butler SC, Chairman)*, Brisbane.
- Community Law Reform Committee of the Australian Capital Territory 1995, *Security Protection and Investigative Industries in the ACT*, Publications and Public Communication, Canberra.
- Critical Infrastructure Assurance Office 2000. *Practices for Securing Critical Information Assets*, [cited 8 June 2000], available online: <URL:<http://www.ciao.gov>>.
- Department of Communication and Information, Local Government and Planning, Queensland. 1999, *Information Standard 16: Management, Agency Information Steering Committees* [cited on 20 April 2000], available on the Internet: <URL:<http://www.dclipg.qld.gov.au/comminfo/download/is16.pdf>>.
- 1999, *Information Standard 24: Information Management, Policies for the Management of Information within Government*, [cited on 20 April 2000], available online: <URL:<http://www.dclipg.qld.gov.au/comminfo/download/is24.pdf>>.
- Department of Consumer Affairs, New South Wales 1993, *Review of private investigation industry: A discussion paper*, Sydney.
- Fitzgerald Report 1989 — See *Report on a Commission of Inquiry Pursuant to Orders in Council*.

- Independent Commission Against Corruption 1992a, **Report on the unauthorised release of government information**, Vol. 1, 2 & 3, ICAC, Sydney.
- 1992b, **Just Trade: Proceedings of a seminar on the ICAC Report on the unauthorised release of government information**, ICAC, Sydney.
- Legal, Constitutional and Administrative Review Committee 1998, **Privacy in Queensland, Report No. 9**, Legislative Assembly of Queensland, LCARC, Brisbane.
- National Police Research Unit 1995, **A Standard Law Enforcement Information Security System: Guidelines for Law Enforcement Agencies**, restricted circulation, NPRU [now known as the Australasian Centre for Policing Research], South Australia.
- 1994, **Improper Access and Use of Confidential Information by Police**, NSW Ombudsman, Sydney.
- 1995, **Confidential Information and Police**, NSW Ombudsman, Sydney.
- Organisation for Economic Co-operation and Development 1992, **Guidelines for the Security of Information Systems** [cited 6 August 2000], available online: <URL:http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/secur.htm>.
- Police Education Advisory Council 1998, **Police for the Future: Review of Recruitment and Selection for the Queensland Police Service**, Criminal Justice Commission & Queensland Police Service, Brisbane.
- Prenzler, T., Baxter, T. & Draper, R. 1998. 'Special Legislation for the Security Industry: A Case Study', **International Journal of Risk: Security and Crime Prevention**, vol. 3, no. 1, pp. 21–33.
- Prenzler, T., Draper, R. & Harrison, A. 1996, 'The Case for Non-police Private Security', **Journal of Security Administration**, Vol. 19, No. 1, pp. 16–33.
- Prenzler, T. & Hayes, H. 1999, 'An Evaluation of the Queensland Security Providers Act: Implications for National Regulation of the Protective Security Industry', **The Australian and New Zealand Journal of Criminology**, vol. 32, no. 1, pp. 79–94.
- Prenzler, T. & Sarre, R. 1999, 'A Survey of Security Legislation and Regulatory Strategies in Australia', **Security Journal**, vol. 12, no. 3, pp. 7–17.
- Prenzler, T. & Sarre R. 1998, 'Regulating Private Security in Australia', **Trends and Issues in Crime and Criminal Justice**, vol. 98, pp. 1–6.
- Report on a Commission of Inquiry Pursuant to Orders in Council [Fitzgerald Report] 1989**, Government Printer, Brisbane. Title of Inquiry: Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct [Fitzgerald Inquiry] 1989, Chaired by G E Fitzgerald, QC.
- Sarre, R. 1994, 'The Legal Powers of Private Police and Security Providers', in **Private Prisons and Police: Recent Australian Trends**, chapter 12, pp. 259–80, edited by P Moyle, Pluto Press, New South Wales.
- Sarre, R. 1998, 'Accountability and the Private Sector: Putting Accountability of the Private Security under the Spotlight', **Security Journal**, No. 10, pp. 97–102.

- Standards Australia & New Zealand Standards 2000, HB231:2000, Information security risk management guidelines, Standards Australia, Strathfield.
- 1999, AS/NZS4444.1:1999, Information security management, Part 1: Code of practice for information security management, Standards Australia, Strathfield.
- 1999, AS/NZS4444.1:1999, Information Security Management, Part 2: Specification for Information Security Management Systems, Standards Australia, Strathfield.
- 1999, AS/NZS4444.2:1999, Information Security Management, Part 1: Code of Practice for Information Security Management, Standards Australia, Strathfield.
- 1999, HB143:1999, Guidelines for Managing Risk in the Australian and New Zealand Public Sectors, Standards Australia, Strathfield.
- Swanton, B. 1993. 'Police and Private Security: Possible Directions', *Trends and Issues in Criminal Justice*, No. 42, pp. 1–8.

Further Reading

- Australian National Audit Office 1998, Protection of confidential client data from unauthorised disclosure: Audit Report No. 37 of 1997–98 [cited 9 June 2000], available from Internet: URL:<http://www.anao.gov.au>>.
- Bartholomew, P. 1997, 'Disclosure of Official Information: The Criminal Law Amendment Bill 1996', *Legislation Bulletin*, No. 3/97, Queensland Parliamentary Library, Brisbane.
- Board of Governors of the Federal Reserve System 1997, Sound practices guidance for information security for networks [cited 8 June 2000], available online: URL:<http://www.federalreserve.gov/boarddocs/SRLETTERS/1997/SR9732.HTM>>.
- Button, M. 1998, 'Beyond the Public Gaze — The Exclusion of Private Investigators from the British Debate over Regulating Private Security', *International Journal of the Sociology of Law*, vol. 26, pp. 1–16.
- Civil Service Department 1979, *Disclosure of Official Information: A Report on Overseas Practice*, United Kingdom.
- Clarke, R. 1992, Practicalities of Keeping Confidential Information on a Database with Multiple Points of Access: Technological and Organisational Measures [cited 23 June 2000], available online: <URL:<http://www.anu.edu.au/people/Roger.Clarke/DV/PaperICAC.html>>.
- Commonwealth Ombudsman 1995, *Own Motion Investigation into the Improper Accessing of Information by Members of the Australian Federal Police*, Australian Government Publishing Service, Canberra.
- Crider, W. 1998, 'Using Oracle Tools to Audit Oracle Logical Security', *Audit & Control Journal*, vol. iv, pp. 15–22.
- Criminal Justice Commission 1994, *Selling Your Secrets*, Issue Paper Series, vol. 1, no. 1, Brisbane.
- Critical Infrastructure Assurance Office 2000. *Hearing before the Senate Judiciary Committee. 2000. Statement of John S. Tritak, Director, Critical Infrastructure Assurance Office* [cited 7 February 2000], available online: <URL:http://www.ciao.gov/Testimony/02_01_00.Tritak.htm>.

- Finn, P. 1991, *Official Information: Integrity in Government Project — Interim Report I*, Australian National University, Canberra.
- Gill, M. & Hart, J. 1997, 'Exploring Investigative Policing: A Study of Private Detectives in Britain', *British Journal of Criminology*, Vol. 37, No. 4, pp. 549–67.
- Grace, R. 1996, 'Computer Technology and Criminal Investigation: Two Decades of Progress', *Journal of the Queensland Police Service*, No. 164, pp. 8–9.
- HM Inspectorate of Constabulary 1999, *Police Integrity: Securing and Maintaining Public Confidence*, Swindon Press, London.
- Hatte, P. & Shiels, M. 1996, 'Private Policing — The Security Industry', *Policing Issues & Practice Journal*, April, pp. 14–21.
- ICAC 1994, *Investigation into the Relationship between Police and Criminals — First Report*, Sydney.
- 1994, *Investigation into the Relationship between Police and Criminals — Second Report*.
- 1994, *Report on Investigation into Matters Relating to Police and Confidential Information*.
- 1994, *Implementation of Recommendations from the ICAC Investigation into the Relationship between Police and Criminals (Milloo)*.
- *Managing Post-separation Employment – Discussion Paper* [cited 10 April 2000], available online: <URL:http://www.icac.nsw.gov.au/pub_corruption_prevention/pub2_25_0cp.htm>.
- *Internal Reporting Systems* [cited 10 April 2000], available online: <URL:http://www.icac.nsw.gov.au/pub_corruption_prevention/pub2_18_0cp.htm>.
- Federal Privacy Commissioner (Australia) 2000, *National Principles for the Fair Handling of Personal Information* [cited 22 July 2000], available online: <URL:<http://www.privacy.gov.au/private/index.html>>.
- Jackson, M. 1993, 'Unauthorised Release of Government Information', *Computer Law*, Vol. 1, No. 2, pp. 54–59.
- Jones, A.. 1997, 'Penetration Testing and System Audit — Experience Gained during the Investigation of Systems within the UK', *Computers & Security*, No. 16, pp. 595–602.
- Osbourne, K. 1998, 'Auditing the IT security function', *Computers & Security*, No. 17, pp. 34–41.
- McConnachie, A. 1999, 'New Privacy Legislation for New South Wales', *Law Society Journal*, March, pp. 58–60.
- Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000, *Discussion Paper. Model Criminal Code. Chapter 4. Damage and Computer Offences and Amendment to Chapter 2: Jurisdiction*, Attorney-General, Canberra.
- National Computing Centre, 1996, *The Information Security Breaches Survey*, United Kingdom.

- Office of the NSW Ombudsman 1997, *Conflict of Interest*, Sydney.
- 1997, *Conflict of Interest and Police: A Service-wide Problem*, Sydney.
- Parkin, R. K. 1998, 'The Importance of IT security', *Computer Fraud & Security*, March, pp. 12–15.
- Polk, K. & Ranson, D. 1991, 'The Role of Gender in Intimate Homicide', *Australia and New Zealand Journal of Criminology*, No. 24, pp. 15–24.
- Smith, M. 1998, 'Security — Who cares?', *Computer Fraud & Security*, April, pp. 12–15.
- Standards Australia 1999, HB142:1999, *A Basic Introduction to Managing Risk*, Strathfield.
- United States General Accounting Office 1998, *Executive guide: Information Security Management – Learning from Leading Organizations*.
- 1999, *Information Security Risk Assessment. Practices of Leading Organizations (a supplement to Executive Guide: Information Security Management)*.
- Warren, I. 1995, 'An Air of Uncertainty: Private Security Regulation in Victoria', *Deakin Law Review* 2/2, pp. 223–53.
- Wilson, P., Keogh, D. & Lincoln, R. 1994, 'Private policing: the major issues', in *Private Prisons and Police: Recent Australian Trends*, chapter 13, pp. 281–98, edited by P Moyle, Pluto Press, New South Wales.
- Wood, J.R.T. 1997, *Royal Commission into the New South Wales Police Service Volumes I, II, III*, the Government of the State of New South Wales, Sydney.