E-policing:

The Impact of Information Technology on Police Practices

Janet Chan • David Brereton • Margot Legosz • Sally Doran

September 2001

ISBN 1 876986 01 8

Criminal Justice Commission
Level 3 Terrica Place
140 Creek Street, Brisbane, Queensland, Australia

Tel.: (07) 3360 6060

Fax: (07) 3360 6333

E-mail: mailbox@cjc.qld.gov.au

Note: This publication is accessible through the CJC website — www.cjc.qld.gov.au.

Contents

Acknowledgments

This study was conducted by the School of Social Science and Policy at the University of New South Wales in partnership with the Research and Prevention Division of the Criminal Justice Commission. The research was jointly funded by the Australian Research Council and the CJC under the Strategic Partnership with Industry — Research and Training Scheme.

We gratefully acknowledge the cooperation and assistance of the Queensland Police Service and its officers, especially Mr Jim O'Sullivan, former Police Commissioner; Mr Bruce Mortimer, former Manager of Information Planning Branch; Mr Denis Luttrell, Director of Information Management Division; and a number of Assistant Commissioners for facilitating the research process. We also thank all participants in the study, including officers who took part in the surveys, focus groups, interviews and those who consented to being observed.

Professor Peter Manning and Mr Bruce Mortimer acted as external reviewers of the report.

Others who assisted with the project include: Tara McGee, Lisa Evans, Terri McTegg, Jodie Boland and Gabi Hoffmann from the Criminal Justice Commission. Transcription of interviews was done by Bev Loughton and Karen Monkerud. The authors are grateful for their assistance.

Dr Janet Chan
Associate Professor and Head of the School of Social Science and Policy, University of New South Wales

Dr David Brereton
Director, Research and Prevention Division, Criminal Justice Commission

Dr Margot Legosz
Research Officer, Research and Prevention Division, Criminal Justice Commission

Sally Doran
Research Assistant, School of Social Science and Policy, University of New South Wales

Abbreviations

ABCI	Australian Bureau of Criminal Intelligence
ABS	Australian Bureau of Statistics
ACID	Australian Criminal Intelligence Database
ARI	Activity Report Index
AVL	Automatic Vehicle Location
BCIQ	Bureau of Criminal Intelligence Queensland
CAD	Computer-aided dispatch
CBT	Computer-based training
CJC	Criminal Justice Commission
CJIIS	Criminal Justice Information Integration Strategy
CITEC	This is the Queensland State Government computer and information agency.
COP	Commissioner of Police
COPS	Computerised Operational Policing System
CRIMS	The Crime Reporting Information Management System
CRISP	Crime Reporting Information System for Police
CRS	Crime-reporting system
DETO	District Education and Training Officer
DNA	Deoxyribonucleic acid
EAGLE	NSW police information system named after the Service emblem, the Eagle.
EEO	Equal Employment Opportunity
e-mail	Electronic mail
ESC	Ethical Standards Command
FG	Focus Group
FOI	Freedom of Information
FYC	First Year Constable
GD	General Duties
ID	Identity
IITP	Investigations and Intelligence Training Program
IMD	Information Management Division
IMS	Incident Management System
IPB	Information Planning Branch
IRC	Information Resource Centre
ISB	Information Systems Branch
ISC	Information Steering Committee
ISS	Information Security Section
IT	Information technology
MINDA	Mobile Integrated Network Data Access
MIST	Management Information Systems Traffic
MNCR	Metropolitan North Correspondence Register
NAFIS	National Automated Fingerprint Identification System
NEPI	National Exchange of Police Information
NEVDIS	National Exchange of Vehicle and Driver Information System
NTA	Notice to Appear
NVOI	National Vehicles of Interest
OIC	Officer in Charge
OPM	Operating Procedures Manual
PC	Personal computer
PIC	Police Information Centre
POCC	Police Operational Conversion Course
POP	Problem-oriented policing
PROVE	Police Recruit Operational Vocational Education Program
PSMC	Public Sector Management Commission
QPS	Queensland Police Service
QTAOS	Query Traffic Accident Outstanding Supplementary
QUID	Queensland Intelligence Database
RBT	Random Breath Test
RETC	Regional Education and Training Coordinator
RETO	Regional Education and Training Officer
RIMO	Regional Information Management Officer
TINA	Ticketable Infringement Notice Automation
TIRS	Traffic Incident Recording System
TRAILS	Transport Registration and Integrated Licensing System
ViCAU	Violent Crime Analysis Unit
ViCLAS	Violent Crime Linkage Analysis System
VIN	Vehicle Identification Number

Report overview

Police have generally responded well to the information technology age. However, this study has shown that, while information technology may have enabled police to do some existing tasks better, it has not yet led to major changes in how the Queensland Police Service (QPS) deals with crime and disorder issues. Our conclusion is that information technology has transformed the structural conditions of policing in the Service in some important ways, while leaving many cultural assumptions and traditional policing practices unchallenged. The experience of the QPS illustrates the more general point that giving police access to computers, increasing the range and quantity of information that is stored electronically and automating what were previously manual processes will not change how the business of policing is conducted by the agency. If police agencies are to get a better return on their investment in IT, there needs to be a conscious and sustained effort to change the organisational settings into which that technology is being introduced. It is very important that the focus of planning for information technology is on assisting policing organisations to get where they should be, rather than simply on streamlining — and thereby entrenching — established practices.

Research questions

This research report analyses the impact of information technology on policing, using the QPS as a case study. It examines the extent to which the implementation of information technology has modified the accountability structure and the occupational culture of policing and whether information technology has significantly altered police practices at the street, supervisory and management levels. More generally, the research explores the potential and limits of technology as a tool for police reform. The major research questions addressed are:

1. How has information technology been received by members of the police organisation? What are the organisational consequences of such acceptance or resistance?
2. To what extent has the introduction of information technology changed the way routine work is conducted by police officers? How does its impact vary

according to functional area (e.g. general duties, traffic, criminal investigation) and geographical location?

3. How does information technology affect supervisory and management practices within the police organisation? To what extent has information technology been used by managers to implement or monitor policy?
4. To what extent has information technology achieved its intended objectives?
5. What impact does information technology have on the level and form of accountability in policing?

A review of the literature shows that there has not been a great deal of research into the impact of information technology on police organisations. The available evidence indicates that information technology has offered a mixture of benefits, led to some fundamental changes and brought with it some unintended consequences. The important message from the literature is that technology should not be seen as purely technical and physical — it can shape social life but is itself modified by social and organisational conditions. The impact of technology on policing is dependent on how technology interacts with existing cultural values, management styles, work practices and technical capabilities.

Research methods

This study was jointly funded by the Australian Research Council and the Queensland Criminal Justice Commission (CJC). The CJC has an ongoing role of monitoring, reviewing, coordinating and initiating reform of the administration of criminal justice in Queensland, including the QPS. It was this association that facilitated access to the QPS for this research. The project was undertaken with the full support and cooperation of the QPS. The report was also reviewed by QPS representatives before its publication.

The methods for this research included a number of interviews and focus groups, a statewide survey, extensive document review, and a series of ride-along observations with police who were attending to calls for service or undertaking traffic duty.

Interviews

Between July and December 1998, a total of 28 people were interviewed in 17 in-depth interview sessions (several sessions included several people). Interviewees included senior police executive and corporate services staff, police and civilian staff members of the Information Management Division (IMD), former IMD staff and consultants to the Division. One participant was reinterviewed in late 2000 to ensure that the information provided on the latest and future developments of information technology was accurate.

Focus groups

Eleven focus groups were held — nine in December 1998, and two in September and November 1999. Samples of operational police, officers in charge and information-management personnel were selected to participate (n = 106).

The survey

The survey of officers was conducted in the first few months of 1999. To ensure a representative sample in terms of rank (First Year Constable to Inspector), job description (including operational and supervisory police) and location (urban and rural areas), three groups of respondents were targeted:

- Police enrolled in training programs at the Academy (in Brisbane and Townsville), Chelmer Police College and Police Headquarters (for the Constable or Management Development Programs, the First Year Constable Program and Domestic Violence legislation training). These respondents were asked to complete the surveys during dedicated class time with the approval of the class supervisor and a full explanation of the purpose of the survey by an officer from the CJC.
- Officers from police stations (such as Beenleigh and Ipswich) who had previously participated in research for the CJC, as well as police officers who currently work at the CJC.
- Officers from a random sample of all rural and remote police stations with a staff of fewer than 8 officers (n = 112 stations, n = 252 officers). Each selected station was sent copies of the survey with a full explanation of its purpose and a reply-paid envelope. It was considered important to ensure adequate rural representation for the survey sample.

In total, 506 officers responded to the survey. The proportions of survey respondents by gender, rank, age and region were generally representative of the Service, with the exception of Constables/First Year Constables, who were over-represented. This anomaly was the result of the specific targeting of respondents through the Academy.

Document review

A large amount of written material (such as annual reports, strategic and implementation plans and program specifications) was provided by the QPS and subjected to extensive review. The QPS Bulletin Board (or intranet) was also found to be a valuable source of information.

Ride-along observations

Initially, a pilot ride-along observation was undertaken by a research officer from the CJC with two general duties officers from an inner-city police station. Later, in

June–July 2000, 8 'half-shifts' of approximately 4 to 4.5 hours duration were observed — one was with an officer from the Traffic Branch, the rest were with officers in cars responding to calls for service. Daytime and evening observations were conducted.

Limitations of the study

During the period in which this research was undertaken, a significant number of changes in information technology were implemented throughout the QPS. While we have made every effort to include the major systems and programs used, we may have missed some of these innovations or changes. Similarly, during the research period a number of senior staff in the IMD either left the QPS or were transferred to other positions; for the most part, it has not been possible to obtain the views of the new staff in those roles.

It is also important to point out that our findings are mainly based on accounts and opinions of officers who participated in the research. These accounts have to be interpreted with caution, as survey respondents and interviewees may have exaggerated or misrepresented what happened. Where possible, we compared accounts from different sources and cross-checked participants' accounts with documentary sources to assess their validity. However, discrepant descriptions of reality often provide insights into structural or situational variations within an organisation.

Finally, there are obvious limitations in conducting a case study on a single police organisation. We cannot claim that the findings of this research are necessarily generalisable to other police organisations. We do, however, try to place these results within the social and organisational context of the case study and assess the extent to which they are likely to be replicated in other police organisations.

Key findings

Development of information technology in the QPS

The development of information technology in the QPS was driven by technological, managerial and policy concerns. The introduction of computer technology in the mid-1970s was modest and haphazard, directed at the information needs of a specific crime problem (vehicle theft). With the advance of information technology, the use of computer systems was expanded over the next two decades to include the processing of data for crime recording and investigation, communication with other government agencies and computer-aided dispatching. Successive attempts to upgrade the information systems were made to redress technical deficiencies identified by

various external inquiries — quality of data, accessibility, lack of integration and various inefficiencies.

By the late 1980s, however, several sources of external pressure had accelerated the push for new and better information technology. The Fitzgerald Inquiry, apart from uncovering serious corruption, was critical of the police force's reactive policing style and rigidly hierarchical management structure. In its final report (Fitzgerald 1989), the Inquiry recommended major reforms to bring about a shift to a community-based, problem-oriented style of policing, as well as more flexible and efficient management practices. The Inquiry also recommended a comprehensive review of QPS information systems to improve the organisation's management capacity.

The establishment of the CJC as the agency responsible for monitoring and reviewing the implementation of police reform in the QPS brought with it additional demands for information for accountability purposes. Accountability requirements of new legislation have also markedly increased the pressure on the QPS to improve its capacity to collect, store and retrieve information. At the same time, the organisation has had to cope with the rising tide of demand for information from various external government and non-government agencies.

The QPS's transition from a low-technology organisation in the early 1980s to the current state of high technology has not been an easy one. One respondent described the QPS of the early 1990s as totally 'immature' as an organisation, not only in relation to information technology, but, more significantly, in relation to management infrastructure following the removal of top levels of management as a result of the Fitzgerald Inquiry. The architects of the information system followed a deliberate strategy of initially securing support for and ownership of the system among operational police, before focusing on managers. The idea was to move gradually from an ad hoc, operationally oriented system to an integrated, tactical, strategic and, eventually, policy-oriented system.

While the QPS has attracted considerable criticism for its management of information technology, it has been under tremendous internal and external pressure to provide a state-of-the-art system that: satisfies legislative and watchdog requirements; is transparent for accountability and auditing purposes; provides accurate and up-to-date statistics to external and internal user groups; and provides an ongoing tool for the day-to-day use of operational police, along with systems capable of superior manipulation for intelligence analysis. However, the large and growing demand for information technology services has not been matched by the levels of funding needed to achieve it. Funding for such endeavours has been insufficient and sporadic.

Practical and technical problems

The introduction of information technology has brought with it a number of practical and technical problems for police. The vast majority of survey respondents told the researchers that they had experienced problems with the information systems 'frequently' (34%) or 'occasionally' (61%). These problems also dominated much of the focus-group discussions.

The most frequently reported problems were associated with the performance of the systems. These ranged from planned or unplanned 'downtime' and access difficulties to software and hardware problems. Focus-group discussions suggested that poor system performance was caused or exacerbated by: the inadequacy of computer equipment, both in availability and in power; the lack of integration of the systems; and severe communications backlog in relation to the QPS Crime Reporting Information System for Police (CRISP). There was also some concern with the accuracy of the data, especially the inconsistent use of CRISP codes, as well as various minor design flaws.

Respondents reported being generally satisfied with the training and support services associated with information technology, although senior officers were less likely to find training adequate and more likely to report satisfaction with support services than junior officers. One notable finding was the high percentage of respondents, especially among the senior ranks, who reported that they learnt to use information technology through informal methods such as 'trial and error' and 'informal help from colleagues', rather than through formal training. It is not clear from the survey whether senior officers did not have adequate access to formal training or they preferred not to make use of the available formal training. We estimated that 1 in 10 officers did not receive any formal training in information technology. This can be due to a number of reasons, including the inability to use computer-based training because of inadequate equipment or poor computer literacy, lack of motivation, time constraints, poor timing, lack of coordination or insufficient time to train staff before the statewide introduction of new technology.

In spite of all the problems encountered, police who participated in the study showed little resistance to the technology. Only a small proportion (16%) reported avoiding some aspects of the systems. In the main, they appeared to have accepted information technology as a useful tool for their work. Far from being Luddites in the Information Age, they saw more powerful, faster and more accessible technology as the answer to their problems. This acceptance signals a potential transformation of the workplace and the organisation as a whole.

Acceptance of technology

Our data show that by the late 1990s information technology had become well accepted and widely used by police in the QPS. Systems such as CRISP were used by 80 per cent of the survey respondents every day or several times a week. The vast majority of respondents thought that technology had made a great difference to police work. This feeling was particularly prevalent among respondents who had had longer service in the QPS and those in higher ranks. In spite of many complaints in the focus groups about various technical problems, QPS officers' assessment of the impact of technology on their own work was generally favourable. The majority of survey respondents indicated that information technology had allowed them to work more effectively, made their work easier and helped them cope with the amount of information police needed to do their work properly. The perception of gain in efficiency as a result of information technology was especially strong among police who had experienced the old technology.

Survey respondents also rated highly the impact of information technology on workplace relations and communication. The majority agreed that information technology had led to improved information sharing and improved communication between workers. Similarly, respondents tended to agree that information technology had allowed people to work more cooperatively and created a better work atmosphere. Improvement in communication between workers was largely the result of the availability of e-mail, which facilitated teamwork, information gathering and information sharing. Information technology was also perceived to have had a good impact on the quality of police service. Six out of 10 survey respondents thought that information technology had led to improved police service to the public and improved police response to crime. Several focus groups mentioned that the crime reporting system had made police procedures more transparent and allowed victims and complainants to get faster feedback on the progress of their case. Our observations also found enthusiastic support from operational police for the mobile data facility that gave police direct access to data on outstanding warrants and vehicles and persons of interest.

Impact on police practices

While information technology may have enabled police to do some existing tasks better — such as recording and following-up on offence details, enforcing warrants and running criminal history checks — it has not yet led to major changes in how the QPS deals with crime and disorder issues.

Less than 40 per cent of the police officers surveyed thought that information technology had led to a more problem-oriented police service or better proactive policing. Some officers in one focus group mentioned the potential for 'intelligence-

driven patrols', 'hot spots' and repeat-offender analysis, and proactive crime investigations, but others were sceptical of the prospects for successful implementation. As one focus-group participant pointed out, information technology may have given police the potential to be more proactive, but they lacked the necessary resources and expertise to realise this potential. Another interviewee observed that the 'technological frame' of traditional police culture tends to see information as useful only if it leads to arrests:

> … even our 'intel' people, even the high-end users, our power users, generally see information from an offender perspective — in other words, information analysis is all about how we can … find an offender … how do you nick someone, and so that limits what becomes useful information. (Senior Information Technology Manager, Interview #1)

According to this interviewee, there was not a clear vision of what problem-oriented policing might offer; it was still seen as 'soft' and marginal. Information technology has, in effect, 'made things easier, rather than made things different'.

Efforts to make the QPS more information-driven have been hindered to some extent by shortcomings in the technical systems themselves: key databases such as CRISP and computer-aided dispatch (CAD) are not linked; some important types of data (such as call histories for particular addresses and repeat victimisation profiles) cannot be readily accessed; output is difficult to interpret because of the lack of standardised, user-friendly reporting functions; and managers cannot readily access timely data on trends and patterns at the local level. Historically, the poor state of QPS information technology systems in the early 1990s meant that the most pressing organisational need was to establish a basic computing infrastructure and core systems such as CRISP and Polaris. It has been difficult for the Service to consider higher-order issues, such as database linkage, and development of management information systems, until these basic elements are in place.

Although the significance of these technical obstacles should not be understated, cultural and organisational factors have also played an important role. Arguably, had there been a stronger commitment within the QPS from an earlier stage to promoting more innovative forms of policing, there may well have been more demands placed on the information technology area — from above and below — to develop systems to support these new approaches.

Recent developments in the QPS indicate that there is now a renewed emphasis on using information to identify and deal with crime and disorder issues. However, as other studies have shown, it is very difficult for police organisations to move from a narrow focus on delivering reactive policing and catching offenders to a broader problem-oriented approach, even where there is strong commitment from the top to implementing change along these lines.

Information technology and accountability

In recent years the QPS, like many other policing organisations, has begun to impose a broader range of accountability controls, often in response to externally generated requirements. For example, new police powers legislation in 1997 and 2000 created substantial additional recording requirements in relation to the conduct of searches, the detention of suspects for questioning, the use of move-on powers, DNA testing, the diversion of minor cannabis offenders and so on. The Service is also in the process of implementing comprehensive recording requirements for personal searches in response to recommendations contained in a recent CJC report on police strip-searching practices (CJC 2000a). In addition, the QPS, as part of its own risk management processes, is expanding the range of information being recorded about police activities (such as police vehicle pursuits, complaints, use of capsicum spray and injuries to officers).

The police officers in our study saw a close association between the greater use of information technology by the QPS and the increased emphasis on accountability. Two-thirds of the respondents agreed that information technology had required them to report on their activities more frequently and made them more accountable for their actions — although several pointed out that it was the need for accountability that caused the additional workload, not the information technology systems. Just over half of the respondents thought that information technology had led to a closer scrutiny of their work by their supervisors and had made their supervisors more aware of their day-to-day activities and workload. Information technology was also seen as having put constraints on police discretion in some areas. About a quarter of survey respondents thought that technology had restricted their discretion, particularly in relation to taking 'shortcuts' in processing cases. A fair proportion (43%) also thought that technology had required police to follow unnecessary steps to get things done. This feeling was particularly strong among detectives and officers in the higher ranks.

Although officers frequently complained that risk management and accountability had gone 'too far', it is possible that they overstated the extent to which their behaviour is now subject to closer scrutiny. Some local bootleg systems have been developed to record information about the workloads and performance of individual officers. Similarly, the CRISP and CAD systems provide a record of officers' actions (or inactions) that can assist in the investigation of complaints and the monitoring of work performance. However, it was evident from focus groups with supervisors that the monitoring capabilities of these systems were not being used — the main explanation offered by supervisors being that they were 'too busy'.

In summary, although police are now being required to record more information for accountability purposes and officers feel that they are under more scrutiny, managers

are still making little use of information technology systems for monitoring and management purposes. The systems themselves have a number of shortcomings, and in some areas risks may have actually increased as a result of the greater ease of access that officers have to confidential information. Consequently, the extent to which there has been a net increase in accountability is very difficult to determine at this stage.

The paperwork issue

Police agencies, like other large bureaucracies, are still very paper-intensive organisations in which substantial amounts of time are spent on completing reports, and considerable organisational resources are expended on administering paper flows and storing and maintaining records. 'Too much paperwork' has been a common source of complaint by police and is often cited by them as an explanation for why they are unable to spend more time on policing tasks such as conducting patrols and investigating crimes. As noted above, managers and supervisors also frequently give this as a reason for not enforcing accountability requirements more strongly.

Information technology has often been held out as providing a solution to the paperwork problem in policing and other bureaucracies by streamlining administrative processes (such as by eliminating the need for multiple forms and multiple entry of data), making information easier to retrieve and reducing the number of hard copy records that must be generated and maintained by organisations. However, many of the QPS officers surveyed said that, as a result of information technology, they now spend more time dealing with paperwork. Respondents in the survey reported spending an average of 3 hours and 37 minutes per 8-hour shift using computers for administrative tasks. Although there are no baseline data from a previous period for comparison, the perception of 4 in 10 survey respondents and many focus-group participants was that the new technology had led to officers spending less time on the street.

Respondents' complaints about the *growing* paperwork and administrative burden need, of course, to be placed in perspective. A fair number of those surveyed occupied supervisory roles, which, by their nature, require them to devote more time to administration and less to operational police work. It is possible that some of these officers may have had difficulty distinguishing between the impact of information technology and the effect of changes in their own role within the organisation. There also may have been a tendency, especially for older officers, to look back to a non-existent golden era of paper-free policing. The historical evidence from Queensland and other jurisdictions strongly suggests that complaints about police being office-bound hardly amount to a recent phenomenon. Without comparable historical data, we simply do not know whether officers are now more immersed in administration

and paperwork than they were before the introduction of information technology. Nevertheless, it is certainly the case that the amount of time being spent on such tasks remains substantial and that the much-touted potential of information technology to streamline administrative processes has yet to be realised.

Information technology may well have the *potential* over the longer term to deliver substantial administrative efficiencies for police organisations by eliminating the duplication of paper and electronic records and the multiple entry of the same data. However, whether this will result in police officers spending less time on paperwork (broadly defined) and more time on the street remains to be seen. One consequence of making it easier for police to collect and process information is also to make it easier for managers and policy makers to request that more be recorded. Hence, any gains in the ease with which specific recording and administrative requirements can be complied with may conceivably be counterbalanced by an increase in the sum total of requirements. It also cannot be assumed that officers will necessarily become more productive once they have less paperwork to deal with: if the time saved is spent in engaging in more conversations with colleagues in the police station, or in conducting additional unstructured mobile patrols, there may prove to be no net increase in policing effectiveness. The ability of police organisations to reap the potential benefits that information technology can bring is heavily contingent on their having the right organisational settings to use this technology effectively.

Police culture

Information technology has created a new form of 'cultural capital' (considered to be a valuable resource in policing) and has also imposed new constraints on police work. Technology has redefined the knowledge and skills required for doing police work. Information, always a valuable commodity in policing, must now be entered, stored and retrieved in a way dictated by the technology. Policing knowledge, which used to be carried inside police officers' heads, has now become synonymous with data that are too complex and voluminous for the human brain to cope with. Officers, especially those in junior operational positions, need to acquire computer skills simply to get their work done. This means that their daily work has become dependent on technology: whether they are able to complete a report, retrieve a piece of information, or get out of the station now depends on whether they have access to a computer, whether the system is 'down', whether the computer is powerful enough and whether they have the skills to use the technology. Thus, information technology has become accepted in the QPS as a necessary resource for policing and IT expertise has become a much valued form of cultural capital.

The growth in funding and staffing of IT-related functions within the QPS was a source of much envy and some bitterness among some officers. The ascendancy of officers with information technology expertise may also have threatened the

traditional power structure of an organisation where previously leaders were predominantly drawn from the criminal investigation branch. Although IT skills have become much valued in policing, some officers were not entirely comfortable with the increased reliance by police on technology for information. They felt that reliance on information technology has meant the loss of local knowledge and the decline of hands-on intelligence gathering.

Information technology has created new cultural divisions and reinforced old ones within the police organisation. One traditional division that has survived, however, is that between management and operational police. Six out of 10 respondents agreed that information technology had led to an overemphasis on accountability. Nearly 4 in 10 also thought that information technology had led to a less trusting or more paranoid organisational atmosphere. A familiar theme among focus-group discussions was that accountability had gone too far, and often at the expense of 'doing the job'. Some officers felt that the Police Service had gone 'risk-management crazy'. They thought that all the auditing and checking was overdone and counterproductive. Some were also concerned with the abuse of technology-generated performance indicators.

Another cultural value not challenged by the new technology is the longstanding resentment that many operational police have against external scrutiny. If anything, this resentment has been justified by the proliferation of indexes and registers that police have to fill out as part of legislative or other accountability requirements. Officers complained that these reporting requirements have made police work more cumbersome.

Our conclusion, therefore, is that information technology has transformed the structural conditions of policing in the QPS in some important ways, while leaving many cultural assumptions and traditional policing practices unchallenged.

Implications for police reform

This study has shed light on the scope for — and barriers to — using information technology as a means of enhancing police effectiveness. The experience of the QPS, while unique in some respects, illustrates the more general point that giving police access to computers, increasing the range and quantity of information that is stored electronically and automating what were previously manual processes will not change how the business of policing is conducted by the agency. If police agencies are to get a better return on their investment in IT, there needs to be a conscious and sustained effort to change the organisational settings into which that technology is being introduced. Effective implementation of intelligence-driven patrolling, for example, requires not only information systems that can provide data on hot spots

and hot times, but also analysts capable of interpreting this information and, most importantly, work allocation systems that will deploy patrols accordingly.

While enhanced information technology may not, of itself, be sufficient to change policing practices, inappropriate technology can often act as a barrier to change. As various studies have shown, there is often a considerable disjunction between the information technology that agencies already have and what they need to support the use of more proactive policing strategies. In the case of the QPS, for instance, the CAD system developed in the early 1990s has been very useful for managing traditional reactive policing activities by facilitating deployment of vehicles, monitoring of work volumes and response times, and so on. However, the current design of the system makes it very difficult to use the data stored in it to identify problem areas and addresses, which in turn has been one of several barriers to promoting the greater use of problem-oriented policing approaches within the QPS.

It is very important that the focus of planning for information technology is on assisting policing organisations to get where they should be, rather than simply on streamlining — and thereby entrenching — established practices. This, in turn, requires that senior managers are able to articulate clearly the management and work practices that they are seeking to implement; that there are structures for ensuring that IT planning decisions are informed by these requirements; and that there is commitment to implementing organisational changes 'on the ground' to promote more effective use of information.

Implications for theory of technological change

The case study sheds new light on the role of cultural factors in understanding the impact of technological change. There was undoubtedly a clash in 'technological frames' (Orlikowski and Gash 1994) between the users and the architects of the systems. Users of the technology, even the more advanced ones, expected it to make their work easier and faster without their having to change existing policing and management styles. Architects of the systems, on the other hand, have intended the organisation to move towards a more sophisticated mode of information usage — for resource management, strategic planning and policy decisions. At the same time, governments and other external bodies have continually demanded that new legislative and accountability requirements be incorporated into the design, so that the capacity and functionality of the systems can constantly be expanded.

Yet the case study has shown that users' technological frames are not immutable. While police resent the additional workload generated by managerial and accountability demands, they have also become willing players in the new technological game. The coercive nature of the technology gave them no alternative.

Thus, despite constant complaints about various technical problems, police have generally responded well to the new technology. Ironically, rather than resisting the burden imposed by the technology, they demand more and better technology in the hope of lightening this burden. If Orlikowski (1996) is correct in saying that organisational change is likely to be emergent and continuous rather than rapid and discontinuous, technology-based organisational change, by gradually and continuously altering the structural conditions of policing, will eventually have an impact on the deeply embedded assumptions of police practice.

Chapter 1: Introduction

Historically, technology has revolutionised police practices. The introduction of the telegraph in the late nineteenth century and the use of two-way radios, motor vehicles and computer-aided dispatching during the twentieth century have brought about dramatic changes in the organisation of police work and, with them, new public expectations of police services. There is, therefore, every reason to expect that the latest round of technological change — the information technology revolution — will have an equally dramatic impact on policing.

Although there is now a growing body of research on technology-based organisational change (see Yates and Van Maanen 1996), the impact of information technology on police practice has not received much research attention. As Manning points out:

> Research on technology has focused narrowly on the managerial potential of the systems rather than on employee morale or performance, control or management of crime, or delivery of enhanced services that improve the quality of community life and citizens' satisfaction with policing. (Manning 1992a, pp. 389–90)

This research aims to analyse the impact of information technology on policing, using the QPS as a case study. It examines the extent to which the implementation of information technology has modified the accountability structure and the occupational culture of policing and whether information technology has significantly altered police practices at the street, supervisory and management levels. More generally, the research explores the potential and limits of technology as a tool of police reform. The major research questions to be addressed in this research are:

1. How has information technology been received by members of the police organisation? What are the organisational consequences of such acceptance or resistance?
2. To what extent has the introduction of information technology changed the way routine work is conducted by police officers? How does its impact vary according to functional area (e.g. general duties, traffic, criminal investigation) and geographical location?
3. How does information technology affect supervisory and management practices within the police organisation? To what extent has information technology been used by managers to implement or monitor policy?
4. To what extent has information technology achieved its intended objectives?
5. What impact does information technology have on the level and form of accountability in policing?

Outline of the report

- Chapter 2 surveys the available literature on the impact of information technology on organisations in general and on police organisations in particular. It also examines the theoretical frameworks used to understand such impact and explores the issues in connection with the use of information technology for police accountability.
- Chapter 3 describes the background to the introduction of information technology into the QPS and outlines the research methods used in this project.
- Chapter 4 provides an overview of the intended objectives of introducing information technology to the QPS, the strategies of development and implementation and the structures and processes established for the management and support of information technology.
- Chapter 5 describes the use of information technology within the QPS and the impact of information technology on operational policing.
- Chapter 6 describes some of the technical and practical problems encountered in relation to the use of information technology.
- Chapter 7 examines the impact of information technology on the police organisation and its relations with external organisations.
- Chapter 8, the final chapter, summarises the findings and outlines the theoretical and practical implications of this research.

Chapter 2:
Literature review

Objectives of information technology in policing

Traditionally, business organisations introduce information technology to further their business goals: to gain a competitive edge, to improve performance, to facilitate new forms of management, or to develop new business potentials (Earl 1989, p. 8). In policing, technological changes are driven by three analogous imperatives: to improve effectiveness and efficiency, to meet the requirements of new forms of police management and accountability, and to satisfy the demand of external agencies for information.

Effectiveness and efficiency

The first imperative is technology-driven. Technology has always had a close affinity with police work. Not only does technology promise to improve police effectiveness and efficiency in controlling crime, it may also enhance their professional status and organisational legitimacy (Manning 1992a; Ericson and Haggerty 1997, p. 390). Given that information is the stock-in-trade of policing, it is natural that police organisations would embrace the latest information technologies. Police are investing in information technology to increase their capacity to store and process large volumes of data; to improve their intelligence and investigative capabilities; and to provide ready access to criminal records and other crime-related information. The need for technology that is compatible with other agencies is also an important driving force for new technology.

New public management and accountability in policing

The second imperative is policy-driven. Police organisations are different from commercial firms in that their use of information technology to improve performance

and management is not driven by market considerations, but is mainly the result of externally imposed demands for public accountability, in terms of cost-effectiveness, probity and procedural regularity. Since the 1980s, a new conception of public accountability has arisen in a number of Western democracies such as Australia and Britain (Davids and Hancock 1998; Chan 1999; Miller and Rose 1990; Power 1997). Traditionally, police practices and procedures are governed by laws and departmental rules that are enforced by the courts and the police hierarchies respectively. The predominant mode of control is deterrence through legislation and rule-making, investigation and enforcement, criminal sanctions and organisational discipline. However, the new accountability for public organisations adopts the managerial techniques and administrative structures of private 'for profit' corporations, emphasising cost control, efficiency, decentralisation of management and cutting back of the public sector, while creating market or quasi-market mechanisms such as contracting out, performance indicators, risk assessment and audit procedures (Power 1997; Chan 1999; Dean 1999). In policing, the new managerialism has transformed the traditional police force into organisations with mission statements, business plans, marketing strategies and a new emphasis on crime management, customer service and performance measures (Chan 1997; O'Malley and Palmer 1996; Leishman, Loveday and Savage 1996). Ackroyd et al. (1992) call it the 'entrepreneurial revolution' in policing. Under this new order, police are being scrutinised *internally* by management systems, surveillance technologies, internal audits and investigations, and *externally* by watchdog agencies, public complaints systems and central auditors, and through the budgetary process. Thus, part of the maintenance and upgrading of information technology in policing is designed to meet the requirements for information under the new management and accountability systems.

External demands for information

The third imperative is information-driven. Apart from meeting the demands of external watchdog agencies for information regarding police actions for accountability purposes, police organisations regularly provide crime and accident data for external bodies such as road traffic authorities and insurance companies. Increasingly, police information is commodified and sold to external commercial institutions and individuals, partly as a cost-recovery measure and partly to discourage frivolous requests (Ericson and Haggerty 1997, pp. 340–5). Thus, these external demands for police information are also partially responsible for the need to improve information technology capacities within police organisations.

The impact of information technology on policing

The use of information technology has become part of everyday life in the twenty-first century for many individuals and the vast majority of organisations. It is, therefore, not surprising that a national mailed survey of US city police agencies in the mid-1990s found that only about 6 per cent did not have an in-house computer system (Mullen 1996). Australian police forces, being typically much larger than American ones, have all adopted some form of Service-wide computerised information system since the mid-1990s. The question of whether the large-scale adoption of information technology has changed police operations, management practices and public service is an important one. Technology certainly has the *capability* to improve efficiency and enhance service, but that this capability is realised in practice is not a foregone conclusion. Unfortunately, there have been very few research studies on the impact of information technology on policing, not only in Australia, but also in other countries (Manning 1992a; Mullen 1996).

Different perspectives have emerged from the available literature on the extent to which information technology has changed police practices. One view suggests that information technologies 'have been constrained by the traditional structure of policing and by the traditional role of the officer' (Manning 1992a, p. 350). Drawing on evaluation studies published in the 1970s and 1980s (e.g. Colton 1978; Rheinier et al. 1979; Chaiken et al. 1975; Hough 1980a), Manning outlined the disappointing results of various technological innovations such as computer-aided dispatch (CAD) systems, attempts to reduce response time, car locator and tracking systems, crime mapping techniques, and management information systems. He concluded that 'such research as exists is often inconclusive or suggests that new technologies have less effect on police practices than their proponents predict or prefer' (Manning 1992a, p. 382).

In contrast, studies in the 1990s came to rather different conclusions. Harper's (1991) research on the use of a computerised crime-reporting system (CRS) by detectives in a medium-sized British police constabulary suggested that information technology had made a clear difference to detective work. Not only had the computerised information system made it easier and faster to access and retrieve information, it had transformed the 'spatio-temporal context in which detectives operate': detectives no longer needed to travel to different places to locate records and they had virtually 24-hour access to files. Although not originally intended by the technology, the CRS gave detectives an advantage over offenders when negotiating about 'offences to be taken into consideration':

> The introduction of the CRS has provided a new device enhancing a detective's ability to bluff. To start with … the system enables the detective to go to an interview much better prepared, with much more information about other possibly relevant offences than in the past. Though this information may not be

> enough to convict, it may be sufficient to persuade the suspect otherwise. In addition, detectives have discovered that by accessing the system while interviewing … their bluffing can be more effective. (Harper 1991, p. 300)

This advantage is likely to be temporary, however, as suspects might eventually get used to seeing computers on the desk of detectives and no longer be intimidated by them.

Ericson and Haggerty's (1997) study of Canadian police organisations, carried out in the early 1990s, demonstrated that information technology had had a profound impact on the way officers thought, acted and reported on their activities. The introduction of information technology meant that individual police discretion was severely circumscribed by the rules, formats and technologies of the reporting systems, whereas supervision had been tightened both prospectively as details of police activities were embedded in the required fields of IT systems and retrospectively as supervisors took more seriously their scrutiny of filed reports. The capability of information technology was such that it had become an effective tool for the surveillance of police supervisors, the detection of misconduct and all types of audits, monitoring and risk management (Ericson and Haggerty 1997, pp. 398–9). The researchers argued that:

> Communication technologies … radically alter the structure of police organization by levelling hierarchies, blurring traditional divisions of labor, dispersing supervisory capacities and limiting individual discretion. In the process, traditional rank structures of command and control are replaced by system surveillance mechanisms for regulating police conduct. (Ericson and Haggerty 1997, p. 388)

According to Ericson and Haggerty (1997, p. 412), information technology has also created new cultures of policing and rendered police organisations more transparent.

The impact of information technology is, however, not always as intended. Ericson and Haggerty (1997) conceded that police officers did actively resist some aspects of information technology through refusal to participate, aversion to use or other forms of subtle resistance. Resistance was likely where officers perceived that such technology was used as a surveillance mechanism by supervisors or where the systems were technically difficult or cumbersome. There were also unintended consequences such as the proliferation of 'bootleg forms', an increase rather than a decrease in paper files and police work becoming even more office-bound in some cases. As Manning (1992a) pointed out, the mere availability and accessibility of information does not necessarily mean that information is used effectively or appropriately by police officers and managers. In general, the use of computer technology may increase productivity without resulting in any gain in efficiency (cf. Henman 1996).

Understanding technological change

To understand the impact of information technology on policing, we need to consider more general theories about technological change and the implications of these theories for policing.

The social context of technological innovation

Researchers who study the impact of technology on social life have long argued that technology should not be seen as consisting of a physical, material dimension only; rather, technology operates in a social context and its meaning is perceived differently by people in different social and organisational positions (Ackroyd et al. 1992; Manning 1992a; Orlikowski and Gash 1994). While technological changes have the capacity to transform social and organisational life, it is important to recognise that technology is itself shaped by social and organisational conditions. This is true regardless of whether the *emergence* or the *impact* of technology is being considered. The development and adoption of a particular technology are rarely governed solely by technical criteria: often they are driven by social, political and moral considerations (Ackroyd et al. 1992, p. 10). Similarly, the impact of a specific technology on social life is often determined by factors beyond its technical capacity — factors that may be psychological, social, political or cultural. Hence, technology may be constraining or enabling, but people have the ability to 'adapt, bend, shape, develop, subvert, misuse and otherwise manipulate technological specifications for various purposes' (Ackroyd et al. 1992, p. 11). Orlikowski and Robey (1991) explained this as the underlying duality (cf. Giddens 1984) of information technology:

> This duality is expressed in its *constituted* nature — information technology is the social product of subjective human action within specific structural and cultural contexts — and its constitutive role — information technology is simultaneously an objective set of rules and resources involved in mediating (facilitating and constraining) human action and hence contributing to the creation, recreation and transformation of these contexts. Information technology is both an antecedent and a consequence of organizational action. (Orlikowski and Robey 1991, p. 151)

Orlikowski has therefore argued that the impact of technological change on organisational structure, work practices, communication channels and performance cannot be understood in a *deterministic* or rationalist way (Orlikowski 1996, p. 64). Instead, the consequences of information technology should be interpreted via an *interpretive* or *emergent* model — that is, that they result from the 'interplay among computing infrastructures, conflicting objectives and preferences of different social groups and the operation of chance' and that information technology is open to interpretation during implementation and use (Robey and Sahay 1996, p. 95). These models stress the active role of organisational members and the importance of social context and processes that produce the meanings of technology. From this

perspective, technology is 'an occasion for, not a determinant of, organisational change' (Barley 1986).

To understand the impact of information technology on organisations, it is important not to simply take a top–down perspective; that is, start with the introduction of IT by management and ask to what extent the original objectives were met. Instead, one should also consider a bottom–up view; that is, start with the goals, strategies and activities of street-level staff who are the users of IT and ask to what extent the technology has facilitated or hindered their work (cf. Sabatier 1986). Only by examining *multiple* perspectives is it possible to fully understand the dynamics of technological change.

Broadly speaking, we can distinguish three types of factors that influence the course of technological change and its impact on organisations: (a) *technical factors,* which include the nature of technology itself and how technological change is managed; (b) *cultural factors*, which include the assumptions inherent in the introduced technology and the extent to which these are congruent with those held by users within organisations; and (c) *political factors*, which consist of the interests at stake in technological change and the conflict or bargaining that may result.

Technical factors

Technological change can have a large or small impact on organisations depending on the nature and design of the technology and the way in which the change is managed.

Studies of 'diffusion of innovation' find that innovations that are successfully implemented share a number of common features: they are compatible with the economic, sociocultural and philosophical value system of the adopter; flexible; reversible; superior to current and previous methods; simple to understand; cost-efficient; easily upgradable; and do not create a high degree of uncertainty within organisations (Rogers 1995). Ericson and Haggerty's (1997) research suggests that information technology has had a substantial impact on policing partly because of the design and implementation of a more *coercive* technology that is difficult to avoid or bypass:

> Communications technologies are designed to compel police officers to use them. When basic occurrence reporting is built into the communication technology, the police officer simply cannot do his or her work without using the technology. Communication technology accentuates the fact that paperwork is the work and cannot be avoided … Resistance … becomes increasingly difficult and sometimes impossible. (Ericson and Haggerty 1997, p. 394)

In fact, where systems are less coercive or less effective, technology can be called upon to correct the problem:

> An information systems manager … said that resistance or simple aversion were ongoing problems, but were about to be corrected by a technological solution: 'There are guys out there that I know for a fact haven't logged on for two years, because we just put in a new payroll system and now they have to log on to put in their overtime and I've seen guys in there that have not logged onto the system for over six hundred days! … '. (Ericson and Haggerty 1997, p. 414)

Diffusion studies show that failures can operate at different levels: technical failure, communication failure, adoption failure, implementation failure and maintenance failure (Orlandi et al. 1997). To minimise the probability of failure, various management strategies have been recommended: increased user participation in all aspects of implementation, the use of 'champions' or 'change agents' to facilitate communication between groups, and adoption of incremental rather than radical change to minimise uncertainty (Orlandi et al. 1997; Howell and Higgins 1990; Rogers 1995; Van de Ven and Rogers 1988). Sparrow (1991) has long emphasised the importance of *managing* information systems properly:

> [I]f badly managed, they can frustrate managerial purposes, enshrine old values, focus attention on outdated and inappropriate performance measures, give power to the wrong people, cast in concrete old ways of doing business, create false or misleading public expectations, destroy partnerships and impose crippling restrictions to new styles of operation — quite apart from their propensity to consume millions and millions of tax dollars. (Sparrow 1991, p. 26)

Examples of technical and implementation problems connected with information technology in policing include flaws in systems design, which result in data of poor quality, and failure to build and maintain support for technology within police departments (Hough 1980b).

Cultural factors

Technology is not simply an objective, physical, given — it has to be interpreted by users and this interpretation explains their interaction with it:

> To interact with technology, people have to make sense of it; and in this sense-making process, they develop particular assumptions, expectations and knowledge of the technology, which then serve to shape subsequent actions toward it. While these interpretations become taken-for-granted and are rarely brought to the surface and reflected on, they nevertheless remain significant in influencing how actors in organizations think about and act toward technology. (Orlikowski and Gash 1994, p. 175)

Orlikowski and Gash (1994) coined the term 'technological frame' to describe a subset of the cognitive schemata shared by members of social groups (Schein 1985; Sackmann 1991). Technological frames can be both helpful and constraining: they can help structure people's experience and reduce organisational uncertainty, but they can also inhibit creativity and reinforce established assumptions (Orlikowski and

Gash 1994, pp. 176–7). Technological frames generally vary between social groups according to the 'purpose, context, power, knowledge base and the [technological] artifact itself' (ibid., p. 179):

> For example, technologists may be expected to have an engineering perspective of technology, treating it as a tool to be designed, manipulated and deployed to accomplish a particular task … In contrast, line managers may have a more strategic understanding of technology, expecting it to facilitate certain ways of doing business and providing financial returns, while users may take a more focused or instrumental view, expecting immediate, local and task-specific benefits. (Orlikowski and Gash 1994, pp. 179–80)

In their case study, Orlikowski and Gash (1994, pp. 183–4) distinguished between three domains of technological frames: (a) the nature of technology — people's understanding of *what* technology is capable of, (b) technology strategy — their view of *why* technology was introduced in their organisation, and (c) technology in use — their understanding of *how* technology is to be routinely used and the consequences of such use. The impact of information technology on organisations can then be explained in terms of the existence of *congruence* or *incongruence* in technological frames between social groups. Where incongruent technological frames exist, the introduction of technology is likely to encounter conflicts and difficulties.

The incongruence between the technological frames of information technology designers and those of the police was evident in the mismatch between the models of policing implicit in the technology introduced in the 1970s and the reality of policing:

> Most attempts to apply analytic techniques such as statistical modelling techniques to police administration are underpinned by a set of assumptions … : (i) the primary objective of the police is crime control; (ii) police activity is one of the primary determinants of crime levels; (iii) the police are organised as a rational bureaucracy; (iv) police strategies are primarily those of deterrence … That these basic assumptions are too inaccurate to pass muster even as a provisional statement is becoming increasingly clear. (Hough 1980b, pp. 351–2)

Such incongruence can create tension in the workplace as workers seek to adjust their practices to conform to the system's requirements:

> … systems designers and implementers very often underrate, or even discount, the working context, its social organisation, its tacit skills and knowledge, into which the system has to fit as a tool of that work. The result is often that working practices must be changed to accommodate to the system in some way (which may or may not be the intention behind the introduction of the system) and/or an uneasy tension is created between those who do the work and the requirements of the system. (Ackroyd et al. 1992, p. 119)

Sparrow (1991) showed the difficulty of trying to make a CAD system designed for traditional-style policing serve a community-based, problem-solving style of policing that management in the Houston Police Department wanted to adopt. Problems of

'call stacking' (holding calls for beat officers to deal with), 'checking by' (allowing patrol cars to do proactive work instead of servicing non-urgent calls), 'call histories' (the amount of time call information should be retained on-line) and 'cherry picking' (officers taking the 'good' calls and leaving the unpleasant ones) revealed the fundamental conflict between traditional-style policing where response time was a major concern and problem-solving policing where police were expected to do proactive work, analyse call histories and make mature, responsible decisions about their work. Sparrow (1991) even warned managers against leaving the design and implementation of information systems to technologists. This example illustrates the incongruence of technological frames between information technology designers and managers. If this example can be extrapolated, where information technology is designed to *change* management culture (Ackroyd et al. 1992), accountability procedures (Ericson and Haggerty 1997) or rank-and-file work practices, clashes in technological frames would exist almost by definition. The result may be various forms of resistance, breakdown in communication or even suspension of the information technology project itself (Orlikowski and Gash 1994, p. 181).

Political factors

Technological changes often 'destabilize the power balance between organizational segments by altering communication patterns, role relationships, the division of labor, established formats for organizational communication and taken-for-granted routines' (Manning 1996, p. 54). Since information itself is a source of power, information technology can lead to power struggles, adaptations or reactions that may subvert the original intentions of the new technology (Orlikowski and Robey 1991, p. 155).

In policing, introduction of information technology can restrict the discretion and autonomy of street-level police officers, while at the same time enhancing the status of IT specialists (Ericson and Haggerty 1997, p. 406). Such developments alter the balance of power between workers and supervisors and between sworn officers and civilians. When officers feel that their autonomy is threatened by internal surveillance or external interference, they are likely to resort to resistance or sabotage where possible. Ericson and Haggerty (1997) gave examples of patrol officers collaborating with dispatchers to avoid being tracked by computer-aided dispatch systems (p. 414) as well as examples of officers refusing or resisting the mandatory reporting of family violence as an 'externally driven surveillance technology based on an outlook of distrust' (p. 386).

Dynamics of technological change

The above discussion may have presented an unduly static view of technological impact. The introduction of new technology is merely the beginning of a

'technological drama' (Manning 1992b; 1996) of normalisation, adjustment, reconstitution and reintegration. When a technology is introduced, efforts are made by management to normalise and legitimise its routine use within the organisation, while the use of alternative technologies or alternative uses of the new technology are discouraged or suppressed. This is followed by adaptive responses such as 'countersymbolization', an attempt by members to devalue or eschew the use of the new technology 'to symbolize their discretion and mark their autonomy from controlling devices'; 'counterappropriation', an inappropriate use of the technology to undermine its intended objectives; and 'counterdelegation', a redefinition of the technology through sabotage or deactivation to maintain discretion and autonomy (Manning 1996, pp. 57–8; Manning 1992b, pp. 337–8). These processes then lead to a technological reconstitution and reintegration where workers and management work out their responses to the normalisation and the adjustment respectively. Reconstitution may involve a change in appearance but not in the underlying principles of work; for example, the gain in efficiency from the use of new technology does not result in any change in the reactive and law-enforcement-focused style of policing (Manning 1992b, p. 339). The resultant reintegration and normalisation may be manifested in various changes as well as continuities in organisational life.

Orlikowski's (1996) 'situated change' perspective of organisational change is also relevant for understanding the dynamic quality of technological impact. Orlikowski offered a view of organisational change that is emergent and continuous rather than rapid and discontinuous:

> … through a series of ongoing and situated accommodations, adaptations and alterations (that draw on previous variations and mediate future ones), sufficient modifications may be enacted over time so that fundamental changes are achieved … Each shift in practice creates the conditions for further breakdowns, unanticipated outcomes and innovations, which in their turn are responded to with more variations. And such variations are ongoing; there is no beginning or end point in this change process. (Orlikowski 1996, p. 66)

Orlikowski's study of the introduction of a call-tracking system of a customer support department in a software company found that the organisational structures and practices of the department had changed considerably over the two years following the implementation of the new technology, but the transformation, 'while enabled by the technology, was not caused by it' (Orlikowski 1996, p. 69). Rather, members of the department 'attempted to make sense of and appropriate the new technology and its embedded constraints and enablements' and through their daily actions and interactions in response to the technology, they enacted 'a series of metamorphic changes in their organizing practices and structures' (Orlikowski 1996, p. 89).

Conclusion

This review of the literature has shown that there has not been a great deal of research into the impact of information technology on police organisations. The available evidence has shown that information technology has offered a mixture of benefits, led to some fundamental changes and brought along some unintended consequences. The important message from the literature is that technology should not be seen as purely technical and physical — it can shape social life, but is itself modified by social and organisational conditions. The impact of technology on policing is dependent on how technology interacts with existing cultural values, management styles, work practices and technical capabilities.

To understand the consequences of the introduction of information technology in police organisations, it is important to examine:

- the nature of the technology itself — how it is designed; what it is intended to achieve; whether it is technology-driven or policy-driven; whether it is compatible with existing organisational values; whether it is simple, flexible, reversible, coercive, superior to current methods and so on
- the way technological change is implemented — whether it is incremental or radical; whether users participated in the design and implementation; whether there is adequate research, planning and testing of the system; how much training and what level of support the users get; whether sufficient resources are available, and whether initial problems were dealt with promptly and satisfactorily
- the extent to which there are clashes in 'technological frames' between designers and users, between managers and operational officers in relation to *what* the technology is capable of, *why* the technology is introduced and *how* the technology is to be routinely used
- the extent to which technological change has changed the balance of power within the organisation in terms of shifting division of responsibilities, opening channels of communication, disrupting existing cultures, restricting discretion, changing management and supervisory practices, and tightening accountability and subjecting officers to surveillance
- the extent to which technology has changed the balance of power between the police organisation and external agencies in terms of opening the police organisation to outside scrutiny, increasing the transparency of decisions, subjecting the organisation to audits and monitoring, and increasing the burden of reporting.

In the next chapter, we describe the background and methodology of a case study that examines the impact of information technology in an Australian police service.

Chapter 3:
A case study — the Queensland Police Service

This chapter provides background information about the QPS and the research methods undertaken for this report, including a description of the interviews, focus groups and surveys undertaken, the respondents, the questions asked and the potential limitations of the methods applied.

Research questions

As outlined in chapter 1, the aims of the project were to determine:

1. How information technology has been received by members of the QPS.
2. The extent to which the introduction of information technology has changed the way routine work is conducted by police officers.
3. How information technology has affected supervisory and management practices within the QPS.
4. The extent to which information technology has achieved its intended objectives and its impact on police accountability.

The Queensland Police Service

The estimated resident population of Queensland for 1999 was 3 515 619, living in an approximate area of 1 734 322 square kilometres. Most of the population is concentrated in the south-east corner and in several moderately sized provincial cities on the coast. The capital city, Brisbane, is located in the south-east. The distance from Brisbane to the northernmost part of the State (the Torres Strait Islands) is approximately 3000 kilometres. The far western regions of the State are more than 1500 kilometres from the capital.

According to the 1999–2000 QPS Annual Report (QPS 2000a), the strength of sworn officers in Queensland at 30 June was 7421 (with 279 recruits in training). There were also 2907 public service staff (such as executive officers and administrative and technical officers) and general employees (such as communications operators, liaison officers, trainees, pilots and tradesmen). The State comprises eight police regions (Far Northern, Northern, Central, North Coast, Southern, South Eastern, Metropolitan North and Metropolitan South) and several commands (such as Operations Support, Ethical Standards Command and State Crime Operations). There are more than 450 police establishments throughout Queensland, ranging from one-officer stations in remote locations to large stations of a hundred or more staff in urban areas.

The QPS has undergone a range of major reforms and restructuring in recent years. The Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct (Fitzgerald 1989) found widespread corruption within both the Police Force and the Government of the time. The report made over 125 recommendations regarding police reform, including the establishment of a watchdog agency, the CJC, to monitor and oversee the QPS. The Fitzgerald Inquiry was critical of the traditional, reactive style of policing in the QPS and recommended a shift to a community-based, proactive and problem-oriented style that would be more sensitive to the needs of individual communities. The Inquiry also identified a number of deficiencies in the management of the QPS, which was inflexible, top–down and rule-bound, and recommended a range of reforms aimed at improving the flexibility and efficiency of management. Fitzgerald's recommendations were accepted by the Government and major structural and procedural changes were implemented. A review by the CJC in 1994 found that the bulk of the Fitzgerald recommendations had been implemented, but that there were still some outstanding issues to be resolved, including the continued reliance on a 'command and control' structure and the lack of incentives for development of problem-solving or innovative policing strategies (CJC 1994, pp. 206–7).

Research methods

This study was jointly funded by the Australian Research Council and the CJC. The CJC has an ongoing role of monitoring, reviewing, coordinating and initiating reform of the administration of criminal justice in Queensland, including the QPS. It was this association that facilitated access to the QPS for this research. However, as a watchdog organisation, the CJC also has an impact on the way the Service operates, which, in turn, is directly related to some of the issues raised in this report. Chapter 4 describes the relationship between the CJC and the QPS in the context of the impact of external demands on the QPS.

The project was undertaken with the full support and cooperation of the QPS; indeed, participants were keen to share their views. This report was also reviewed by the QPS prior to its publication.

The methods for this research included a number of interviews and focus groups, a statewide survey, extensive document review and a series of ride-along observations with police who were attending to calls for service or undertaking traffic duty. Each of these is discussed in detail below.

Interviews

Between July and December 1998, a number of in-depth interviews were conducted. A total of 23 people were interviewed within 17 interview sessions (several sessions included several people). Interviewees included senior police executive and corporate services staff, police and civilian staff members of the Information Management Division (IMD), former IMD staff and consultants to the Division. One participant was reinterviewed in late 2000 to ensure that the information provided on the latest and future developments of information technology was accurate.

Interviewees were requested to provide information on the following topics:

- their main areas of responsibility in relation to information technology
- the major systems for which they held responsibility
- details about each system (such as why each system was designed, who provided input into the design of each system, the costs involved in its development, how each system was implemented and marketed, what training and support mechanisms were provided)
- issues regarding resistance to, or avoidance of, the use of new IT programs
- quality control processes
- the impact and effectiveness of the systems on management and operational police (including communication flow, for example)
- external access to the data collected and generated by the QPS
- ongoing evaluation (problems, shortcomings, unexpected consequences, benefits etc.)
- security issues
- the future of information technology over the next five and ten years.

Focus groups

Eleven focus groups were held — nine in December 1998, and two in September and November 1999. A sample of operational police, officers in charge and information management personnel were selected to participate (n = 106). Table 3.1 provides details.

Table 3.1

Demographic profile of focus-group participants and survey respondents

	Demographic	Per cent of focus-group participants (n = 106)	Per cent of survey respondents (n = 506)
Gender	Male	94	69
	Female	6	21
	Missing information	0	10
Age (years)	21–29	18	44
	30–39	29	29
	40–49	32	14
	50+	21	2
	Missing information	0	8
Highest education level	High school or less	17	30
	Post secondary	34	27
	Some university	16	0
	Degree/post graduate	33	34
	Missing information	0	9
Rank	First Year Constable	0	27
	Constable/Senior Constable	30	42
	Sergeant/Senior Sergeant	28	20
	Inspector and above	36	3
	Civilian	6	0
	Missing information	0	9
Number of years with the QPS	Less than 5 years	8	42
	5–9 years	19	13
	10–14 years	10	11
	15–19 years	14	8
	20 or more years	48	14
	Missing information	0	12
Region	Southern	27	13
	Metropolitan North	16	9
	Metropolitan South	20	11
	South Eastern	5	11
	North Coast	7	7
	Northern	3	11
	Central	5	9
	Far Northern	3	9
	State Crime Operations	10	2
	Other (CJC, ESC, HRD, QCC)[a]	5	12
	Missing information	0	8
Geographical area	Metropolitan	n.a.[b]	31
	Suburban	n.a.	21
	Provincial city	n.a.	15
	Rural	n.a.	25
	Missing information	n.a.	8

Notes

a CJC Criminal Justice Commission
ESC Ethical Standards Command
HRD Human Resource Development, Corporate Services
QCC Queensland Crime Commission

b n.a. Not applicable, information not collected for focus-group participants

The groups included:

- General duties officers from two inner-city stations (FG1: GD [*n* = 7] and FG6: GD [*n* = 10]).
- Officers in Charge (OICs) of a large provincial city (FG2: OICs, *n* = 7).
- OICs of several rural stations (FG3: OICs, *n* = 15).
- Stage 3 detectives in training (FG4: Detectives, *n* = 15).
- Intelligence officers and tacticians from a metropolitan region (FG5: Intel/Tacticians, *n* = 4).
- OICs at a metropolitan region (FG7: OICs, *n* = 4).
- Statewide Regional Information Management Officers (FG8: RIMOs, *n* = 3).
- Detectives, State Crime Operations Command (FG9: Specialist Investigators, *n* = 6).
- District Officers (Inspectors and Superintendents) (FG10: District Officers, *n* = 21).
- Chief Superintendents (FG11: Chief Superintendents, *n* = 14).

Group discussions covered the following issues:

- the types of systems used most frequently and the proportion of time spent accessing each system in a typical day
- the processes of implementation, including program design, personnel involved, consultation and training procedures, problems encountered and the adequacy of resources
- attitudes towards the systems, including avoidance, resistance, support and ease of use
- the impact on the way police work, such as productivity, levels of interest or discretion, types of activities undertaken, reporting procedures and paperwork
- the effect of these systems on supervision or management of staff and the way officers work together as a unit
- the effects on the standard of police work to the public, such as response time or clear-up rates, efficiency and visible presence.

The survey

The QPS and the CJC regularly undertake surveys of randomly selected police officers, usually in the form of a computer-based survey attached to an e-mail message. Given that the response rate for research using this process during the 12 months prior to beginning this project had been in the vicinity of only 20 per cent, and in consideration of other CJC and police research demands, it was decided to

abandon that process for this study. An alternative process was adopted: for the first few months of 1999, specific groups of officers were targeted for inclusion in the survey. To ensure a representative sample in terms of rank (FYC to Inspector), job description (including both operational and supervisory police) and location (urban and rural areas), three sources of respondents were targeted:

- Police enrolled in training programs at the Academy (in Brisbane and Townsville), Chelmer Police College and Police Headquarters (for the Constable or Management Development Programs, the First Year Constable Program and Domestic Violence legislation training) were asked to complete the surveys during dedicated class time with the approval of the class supervisor and a full explanation of the purpose of the survey by an officer from the CJC.
- Officers from police stations (such as Beenleigh and Ipswich) who had previously participated in research for the CJC, as well as police officers who were currently working at the CJC, were asked to complete the survey.
- A random sample of all rural and remote police stations with a staff of fewer than 8 officers (n = 112 stations, n = 252 officers) was selected and each station was sent copies of the survey with a full explanation of its purpose and a reply-paid envelope. It was considered important to ensure adequate rural representation for the survey sample.

Table 3.2 (next page) provides the demographic and organisational profiles of the focus-group participants and survey respondents.

In total, 506 officers responded to the survey. As shown in table 3.2, the proportions of survey respondents by gender, rank, age and region were generally representative of the Service, with the exception of Constables and FYCs, who were over-represented. This anomaly was the result of the specific targeting of respondents through the Academy.

The survey sought answers to:

- how often each information technology system was used (daily, several times a week, once or twice a week, rarely, never)
- how much time was spent using information technology systems during the last shift
- the officers' sense of competency with information technology
- information technology training experiences and satisfaction
- the officers' views on a variety of aspects of the systems (such as ease of use, quality and timeliness of the information, problems with the systems, satisfaction with support services, changes in work practices and overall policing due to information technology).

Table 3.2

Comparison of proportions of survey respondents with Queensland Police Service population by selected demographics

Demographic	Per cent of sample	Per cent of State 1997–98
Gender		
Male		
Commissioned officer	94	95
Non-commissioned officer	94	94
Constable	70	80
Female		
Commissioned officer	6	5
Non-commissioned officer	6	6
Constable	30	20
Rank		
Constable (including FYCs)	57	35
Senior Constable	18	31
Sergeant	14	24
Senior Sergeant	8	6
Inspector	4	4
Region		
Far North Queensland	9	7
Northern	11	7
Central	9	8
North Coast	7	12
Southern	13	9
South Eastern	11	13
Metropolitan North	9	13
Metropolitan South	11	11
State functions (e.g. headquarters)	7	18
External agencies (e.g. CJC)	7	2
Age *(different categories apply)*		***Age***
<25	13	21–25 11
25–29	36	26–30 28
30–34	18	31–35 20
35–39	15	36–40 16
40–44	10	41–45 14
45–49	6	46–50 7
50–54	2	51–55 5
55–60	0.4	56–60 1

Document review

A large amount of written material (such as annual reports, strategic and implementation plans, and program specifications) was provided by the QPS and subjected to extensive document review. The QPS Bulletin Board (or Intranet) was also found to be a valuable source of information.

Ride-along observations

Initially, a pilot ride-along observation was undertaken by a research officer from the CJC with two general duties officers from an inner-city police station. Subsequently, 8 half-shifts of approximately 4 to 4.5 hours duration were observed in June–July 2000 — one was with an officer from the Traffic Branch, the rest were with officers in cars responding to calls for service. Daytime and evening observations were conducted.

The observer either sat in the back seat of the car when there were two officers on duty (in about half of the observations this was behind a built-in safety barrier or cage) or in the passenger seat when only one officer was present. Extensive questioning of the officers was undertaken during the shifts.

The observer stayed with the officers at all times (at the station, in the car and when attending to calls or undertaking speed camera duty, for example), but remained at a safe distance when potentially dangerous situations arose (such as a domestic violence incident and a syringe-wielding offender). No objections were raised by the officers to this process — indeed, many encouraged this up-close experience, inviting direct, hands-on interaction with some equipment (such as speed radar) and introducing the observer to a number of offenders and complainants.

Limitations of the study

A number of limitations of this study must be acknowledged. While we specifically targeted a cross-section of police officers to participate in the focus groups and the survey and are satisfied that we have received a broad range of responses, the respondents were not chosen completely at random statewide. The opinions expressed by these participants are, therefore, not necessarily representative of the opinions of all officers throughout the Service. As mentioned on page 18, the unacceptably low response rates of random surveys undertaken in recent months meant that we could not guarantee an unbiased sample using either method of sampling. However, table 3.2 suggests that the survey sample was generally representative of the officers of the QPS in demographic and employment characteristics.

Another limitation of the study relates to the pace of change in information technology. During the period in which this research was undertaken, a significant number of changes in information technology were implemented throughout the Service. While we have made every effort to include the major systems and programs used, we may have missed some significant innovations or changes. Similarly, during the research period a number of senior staff in the IMD either left the QPS or

transferred to other positions; for the most part, it has not been possible to obtain the views of the new staff in those roles.

It is also important to point out that our findings are mainly based on accounts and opinions of officers who participated in the research. These accounts have to be interpreted with caution because they may have exaggerated or misrepresented what happened. Where possible, we compared accounts from different sources and cross-checked participants' accounts with documentary sources to assess their validity. However, discrepant descriptions of reality often provide insights into structural or situational variations within an organisation.

Finally, there are obvious limitations in conducting a case study on a single police organisation. We cannot claim that the findings of this research are necessarily generalisable to other police organisations. We will, however, situate these results within the social and organisational context of the case study and assess the extent to which they are likely to be replicated in other police organisations.

Chapter 4:
Development of IT in the QPS — an overview

This chapter describes the way information technology systems have been developed, introduced and managed in the QPS. It also details the internal and external pressures that have shaped the development of these systems.

Background

Information technology in the QPS had humble beginnings. Concerns about widespread vehicle theft in 1975 led the then Queensland Police Force to install two computer terminals that had access to the SUNCORP computer system and statistical data on vehicle claims. Between 1975 and 1989 the number of terminals installed in police stations around the State increased from two to 483.[1] Initially, however, 'it was in a pretty sorry state … there was a sort of haphazardness of the way things went' (Interview #12) and 'a fair bit of [computer] training and development happened through osmosis rather than through planned initiatives … some police officers were using their own computers on the job' (Interview #11).

Other technological advances during that period included:[2]

- a Statewide Message Switching System that was commissioned in 1980 through the State Government computer and information agency (CITEC) and offered police an alternative to telephone communication

1 One interviewee commented that Apple computers were installed ('sprinkled') around the State for administrative purposes, but that additional information technology resources were left up to the regions — some Assistant Commissioners bought a lot of equipment, others were less interested and spent the funds on alternative resources (such as staff overtime). 'Both approaches have now ended up with their own problems … the ones that had lots of computer equipment — that equipment's very old and requires a lot of maintenance and they don't necessarily have the budgetary discretion to replace it. Those who bought very little have never really caught up'.

2 Much of this summary comes from an article written by Rebecca Grace (undated) of the QPS.

- the availability of vehicle registration details from the then Main Roads Department through Police Department terminals in 1982
- the formation of a Police Computer Branch in 1983
- the installation of an ICL Super Dual 2958 mainframe in 1984 — three existing police systems (the 'Message' and 'Stolen Vehicle' systems and registration details) were reprogrammed and transferred to the mainframe
- an upgrade of the mainframe in 1985 (Super Dual 2966) and again in 1986 (ICL 3980)
- the introduction of other applications between 1985 and 1987, such as the 'Criminal Names Index' (later updated to 'Persons of Interest'), the 'Personnel' and 'Property of Interest' systems and an online security system
- the introduction of several index systems for the use of specialist sections such as the Fraud, Firearms and Drug squads
- the introduction of a Statewide Criminal Offences Index to record details of offences and court briefs
- the introduction of a Telex Interface which permitted messages to be relayed automatically between the Telex and the computer
- linkages with the Department of Transport were made to enable police to query details of drivers' licences
- QNET satellite transmission was introduced to Queensland
- the introduction of the Persons of Interest System, a Localities Register, Correspondence Indices and Keyholders Indices over 1988–89.

In 1990, CAD was developed by Telecom (now Telstra) for the QPS to aid radio communication and to dispatch jobs to operational police in Brisbane ('it was absolutely brilliant — state-of-the-art stuff at the time it was built', Interview #14, Information Technology Manager). The National Exchange of Police Information (NEPI) was also formed to facilitate linkage of computer systems so that information could be exchanged by police services throughout Australia — NEPI is funded by each individual State based on the number of police per State.

As suggested in chapter 2, technological changes in policing are often initiated to improve effectiveness and efficiency, to meet the requirements for accountability, and to satisfy the demands of external agencies for information. Technological change in the QPS was similarly shaped by these imperatives.

The need for improvement

Successive government inquiries have identified major deficiencies in the QPS's information systems. In the late 1980s, the Fitzgerald Inquiry (Fitzgerald 1989, pp. 268–73) found that information management in the QPS was characterised by poor quality data, inadequate systems, and inaccessible and inadequate processes. The report was highly critical of the then Police Force's capacity to capture, store, retrieve, analyse and report basic data believed to be necessary for the efficient management of modern policing, and was most critical of the inability of information systems to link items of related data. Fitzgerald recommended a comprehensive review of police information systems.

Some years later, the Public Sector Management Commission Review (1993, pp. 215–43) found that access to information services in the QPS was still inadequate, training for information services was poor, and information services were fragmented and uncoordinated. It found that: (a) the information management and technology directions were not linked with the corporate plan; (b) the systems were not owned by operational areas and integrated into operational activities; and (c) that approximately half of the Service's 327 stations had no direct access to systems providing basic police information such as persons of interest (offenders, those wanted on warrants etc.), vehicles and property. The review also found that information was not shared amongst officers and was not generally used to support the management of policing (Mortimer 1998).

In 1994 the CJC conducted a review of the response to the Fitzgerald Inquiry recommendations by the QPS (CJC 1994). While acknowledging that the QPS had undertaken a major overhaul and reorientation of its information management practices, outstanding issues highlighted by the report included a lack of networking, limited access to computing facilities, inadequate computer training, fragmented policies on information management issues, difficulties in providing coordinated computing support, and, most importantly, difficulties in providing accurate, recent and local information at a divisional level.

In 1996 the incoming Coalition Government established a review of the QPS under the chairmanship of Sir Max Bingham. That review recommended that the highest possible priority be given to the Polaris project (an integrated police information system) to ensure adequate transfer of information between it and other criminal justice systems, and that information should be available in a consistent and accurate fashion throughout the QPS (Queensland Police Service Review 1996, pp. 88–90).

The Service responded to the concerns of successive inquiries by:

- including improved technology as a priority strategy for the Service in its 1990–95 Corporate Plan — the development of a suite of integrated systems was proposed
- purchasing desktop computers for every police establishment in the State from special funding provided by the Government in 1991–92 for the implementation of information technology infrastructure and new information systems
- developing the framework for the 1992–96 Information Strategic Plan through wide consultation — funding was established and the plan was largely implemented. In 1995 a new five-year Information Strategic Plan (QPS 1995–2000) was developed and implemented
- establishing the IMD in 1993 to provide a cohesive focus for information technology within the organisation
- developing a number of new information systems specifically for the implementation of integrated operational policing systems and systems to support legislative reforms (such as the proposed new Criminal Code) — the allocations specifically targeted the implementation of statewide data communications (achieved in 1995) and a modern computer infrastructure
- implementing in 1997 a new community policing strategy that placed emphasis on problem solving as a core strategy for crime prevention and community policing — one of the core interdependencies suggested by the strategy was between accurate and timely information and police action
- using information technology systems to monitor police performance, undertake audits, review in-service training, and undertake routine surveillance and customer satisfaction surveys to identify high-risk individuals and situations
- increasing information security to give effect to the requirement that officers are not to make any unauthorised, improper or unlawful access or use of any official and confidential information available to them in the performance of their duties.[3]

However, progress has been measured and some concerns remain. The QPS's own planning documents clearly indicate an awareness of the problems facing

3 Depending on the type of activity, any such activity could lead to disciplinary processes such as:
- conspiracy under the Criminal Code
- charges under s.10.1 of the *Police Service Administration Act 1990*
- breaches of s. 10.12: 'Improper access or use of QPS information' of the Code of Conduct
- breaches of the Commissioner's directions issued under s.1.10 'Release of information' of the Operational Procedures Manual
- where a member suspects that improper access, use or disclosure of information has occurred, they are to report the matter in accordance with established reporting procedures for suspected misconduct pursuant to s. 7.2 of the *Police Service Administration Act 1990*.

information management and the difficulties attending their resolution. The needs assessment summary of the Information Strategic and Infrastructure Plan (1995–2000), for example, highlighted the most important information services and systems problems for the QPS to the year 2000 as:

- the lack of integrated information systems for operational police
- the poor quality data and information services for many mission-critical processes
- the poor ability to exchange information with other related State and national agencies
- poor integration between voice, radio and data communications
- multiple entry of the same data
- the need to access multiple databases to retrieve related information
- the linking of corporate services systems with whole-of-government directions
- the limited ability to analyse information because of its disparate locations
- the timeliness and quality of data capture
- the security of information, information systems and information usage.

The Plan also identified weaknesses in attracting and retaining staff with relevant expertise, insufficient funding, and the poor state of radio communication facilities. The 1998 Client Survey and Service Quality Report (QPS 1998b, p. 30) indicated that improvements in the integration of systems, more computers, access to external information and mobile systems, and less downtime are important to operational police. A review by Mortimer (1998) described other concerns:

- that information is overloading operational police (e.g. Commissioner's Circulars)
- that information systems are not being developed sufficiently to provide for the needs of operational police
- that the levels of expertise of operational police in using the systems are generally poor
- that operational police are increasingly dependent on computer systems, which makes them particularly vulnerable to computer failure ('when the computer's down, that's the end of the job').

It should be acknowledged, however, that the issues confronting the QPS are the same as those that all large police organisations around the world must deal with — in fact, many of the research participants in this study believed that the QPS may, indeed, be well ahead of many of those services with regards to information technology, especially other services throughout Australia ('we blow them away — fair dinkum', Interview #14). As one interviewee stated, 'the Service has reached —

or is starting to reach — a maturity level where it realises that information is terribly important to the way it does business' (Senior Information Technology Manager, Interview #10).

Accountability requirements

Legislation

There are hundreds of Acts of Parliament that contain specific requirements regarding the management of particular categories of information. Failure by government agencies to comply with the requirements of these Acts may in some cases be a criminal offence, involve the government in lengthy and costly litigation or may prejudice the rights of individual citizens and organisations. The information collected by the QPS, in particular, is often required for court, for administrative review, for FOI applications, for Royal Commissions, parliamentary and departmental inquiries, and for investigations carried out by organisations such as the CJC. Examples of such requirements include:

- The QPS is legally bound to maintain audit trails as a result of the following legislation: the *Evidence Act 1977–79*, *Police Service Administration Act 1990*, *Libraries and Archives Act 1988*, and *Financial Administration and Audit Act 1977*.
- The 1996 weapons licensing laws required the development and implementations of a weapons index[4] and the new domestic violence laws released in 1999 required the development and implementation of computer-based training (CBT) packages for training and an upgrade of the Domestic Violence Index. Accountability measures have also led to the implementation of the drugs index, exhibit numbers and such like.
- Major new police powers legislation came into force in Queensland on 6 April 1998 with the proclamation of the *Police Powers and Responsibilities Act 1997*. One important feature of the new legislation was the introduction of an alternative way of starting criminal proceedings. Instead of arresting and charging a person, or serving a summons, police may now issue a notice, similar to an infringement notice, called a Notice to Appear (NTA), which requires the defendant to appear in a nominated court on a designated date (CJC 1999). According to one senior police officer, this Act 'has changed our whole structure or function' (Interview #8). With regards to information technology, it led to the development and implementation of a number of new indexes, such as the Custody Index. The new *Police Powers and Responsibilities*

4 This legislation followed the Port Arthur tragedy — licences were not previously required in Queensland. The Act required the issue of 300 000 licences in the first year.

Act 2000 amended the 1997 Act to provide new powers to police (such as pre-court diversion of minor drug offenders, DNA profiling procedures and dealing with property held by police) and to improve some sections of the Act that were causing operational difficulties (such as move-on directions, NTAs, searching without a warrant and recording of identifying procedures). A number of these new powers were associated with changes to police registers and, in particular, modifications to the Custody Index.

- The *Freedom of Information Act 1992* subjects all official police documents, including relevant e-mail, to scrutiny. The Service's Freedom of Information Unit now receives more FOI applications than any other government department (QPS 2000b *Environmental Scan*).
- The *Financial Management Standard 1997* places restrictions and limitations on the way information is collected, stored and retrieved and the *Public Service Management and Employment Act 1988–90* outlines how proper records are to be maintained. The *Libraries and Archives Act 1988* outlines how complete and accurate records of the activities of the public authority are to be made and preserved.[5]
- Information Standard 24 (Department of Communication and Information, Local Government and Planning, Qld, 1999a) creates government policy that instructs all agencies to develop practices and policies that embrace eight principles: accountability, information exchange, information accessibility, compliance with legal and administrative requirements, information preservation, business continuity, privacy and confidentiality, and preservation of copyright and other intellectual property.

External watchdog: the Criminal Justice Commission

The CJC was established in 1989 by an Act of the Queensland Parliament following a recommendation of the Fitzgerald Inquiry. Under the Act, the CJC is charged with monitoring, reviewing, coordinating and initiating reform of the administration of criminal justice in Queensland, including the QPS. The CJC has, since its inception, held concerns for the lack of integration of systems and the improper access to and/or release of confidential and/or personal information from the QPS computer systems by members of the QPS. A number of reviews have documented these concerns — some have already been mentioned (such as the Fitzgerald Inquiry and the Bingham Review). Others include:

5 A recent QPS report concluded that the Service presently devotes a disproportionate level of resources to ensuring the security and archiving of information held on its various systems and databases. The Polaris system, for example, holds approximately 30 times as much data for the purpose of audit as for use in day-to-day policing activities. The Service is subject to legislation that requires accurate records of all information held on its systems to be maintained for up to 75 years (QPS 2000b).

- *Police and Drugs: A Report of an Investigation of Cases Involving Queensland Police Officer*s (CJC 1997a), which recommended that 'those responsible for the management of the QPS computerised information system urgently consider:
  (a) the insertion of a screen that requires the person accessing data to state the purpose for which the check has been made and, if the check is made on behalf of another person, the identity of that person and that person's userid and
  (b) establishing a full audit trail for e-mail'. The report also observed that the use of e-mail on the police computer system 'provides a regular means of communication between police for apparently improper purposes'.
- *Police Strip Searches in Queensland: An Inquiry into the Law and Practice* (CJC 2000a), which recommended that 'as a matter urgency, the QPS should address problems experienced by QPS officers in accessing and using the Custody/Search Index' (recommendation 6.12).
- *Protecting Confidential Information* (CJC 2000b), which focused on a number of complaints received by the CJC during 1998 and 1999 regarding the unlawful disclosure of confidential information. This review included a public inquiry into the nature of these complaints. Evidence was presented of numerous breaches of information security by a number of police officers. These breaches included the provision of confidential information from police systems, such as Polaris and CRISP, to private investigators and private citizens. As a consequence, some individuals who were registered on those systems were put at risk.[6] 'As a result, 13 officers were disciplined and another resigned. A number of other officers who were suspected of similar misconduct had resigned or retired prior to the commencement of the investigation' (CJC 2001a). This report made recommendations that represented both an organisational and a technological response to the issues and problems identified.

External data requests

Information between agencies is a two-way street. QPS staff often require information from other agencies for investigative purposes,[7] and other agencies seek

6 For example, a Senior Constable was found to have confirmed to an unauthorised third party the existence of a domestic violence order on a woman's file and to have released her silent number to that third party. The woman said that the person who was given the number had been stalking her for years and that she had deliberately kept her whereabouts a secret.

7 For example, QPS staff frequently seek information from external bodies such as:

- Australian Customs
- Australian Securities Commission
- Australian Securities Intelligence Organisation
- Australian Taxation Office
- Australian Bureau of Criminal Intelligence
- Residential Tenancies Authority
- Energex/Ergon Energy
- Department of Justice
- Telecommunications information, such as the online telephone directory, names to numbers, numbers to names, silent/restricted numbers
- National Crime Authority
- International inquiries through Interpol
- Centrelink
- Queensland Fisheries Management Authority
- Interstate Law Enforcement Agencies.

police data for a variety of reasons. The Police Information Centre (PIC) is responsible for the release of documents that have been produced as part of the prosecution process or are derived from criminal history information. Applications for a Court Brief (QP9) or Record of Charges can be made directly to the PIC and applications for a Criminal History or Police Certificate can be made at any police station.

> These services have recently been expanded with the introduction of new legislation by the Children's Commission that provides for the screening of employees in child-related employment. Furthermore, requests for statistics by private lawyers, under the provisions of freedom of information, have increased dramatically and are time-consuming and expensive to execute — indeed, they have the potential to be big business, and the QPS is currently assessing how they will handle such demands (Interview #10).

On the other hand, Property Crime Reports (from CRISP) and Traffic Incident Reports (from the Traffic Incident Recording System [TIRS]), are available from CITEC.[8] This organisation receives all requests for information contained in police property crime report records by members of the public and external organisations, and refers any request for information that requires assessment and adjudication to the CRISP Public Access Liaison Officer of the PIC.

By mid-2000, about 385 clients had been granted access to TIRS: those eligible to apply for access include insurance companies, legal firms, loss assessors and mercantile agents. Thirty-three clients have been granted access to CRISP, with the majority being insurance companies. To be granted access to either system, the business and the individuals in the business must complete a confidentiality agreement, and any searches undertaken can be subject to random audits by the QPS (CJC 2000b).

QPS staff are also permitted to provide some information to the public and external agencies, provided that reference to the particulars of any person, proposed action or

---

8 Through TIRS, authorised users have access to the following details regarding traffic incidents:
- 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 regarding property crimes such as:
- summary of crime details (e.g. crime number, address of offence)
- complainants' details
- informant/witness details
- property details
- modus operandi
- other crime classes (i.e. additional crimes committed)
- recovery details of property.

opinion is deleted in cases where the inquirer has not been granted privileged access status by the Commissioner, and that disclosure is not likely to compromise or prejudice any investigation (Operational Management, section 1.10–1.10.5).[9] Clearly, a highly secure, accurate and comprehensive information system is required to make it possible to respond to such requests.

Current and future systems

Polaris

As police became more aware of what information systems could do, requests for new applications increased, resulting in a proliferation of systems, both small and large. These were inevitably stand-alone systems. These systems were maintained on the Service Mainframe and were referred to collectively as the QPS computer system. Whilst fulfilling the required functions, they could not communicate with other systems and required separate searches and data entry. Consequently the systems contained duplicate information.

In the early 1990s, in an attempt to bring all of these systems together, a decision was made to develop one fully integrated system. This system was called Polaris and it was hoped that it would ultimately replace the QPS computer system. Unfortunately, 'packaged solutions' for an integrated system did not exist — either locally or internationally — so the system had to be developed from scratch. As one Information Technology Manager pointed out:

> If you're buying a packaged solution, the place you normally go is the US … but there's absolutely no such animal. Why not? Because there's no such thing as integrated policing in the US … they don't know how many law enforcement agencies they've got over there — in excess of 6000 they think, but they don't know and so any law enforcement agency, whether it be the Sheriff's office or the city or county police or the highway patrol … they've got their own little system and they don't give a rat's about anything else … there's no such thing as integrated policing therefore there's no such thing as [an] integrated system, therefore there's none for us to buy. (Interviewee #14)

9 This includes:
- some information on Queensland vehicle registrations and driver's licence particulars to officers of the Department of Natural Resources (Forest Resources Division) and the Department of Primary Industries (Forestry), but only for the specific purpose of detecting offences against the *Forestry Act*.
- some information about stolen property and facts relating to occurrences of public interest
- any statistics contained in the QPS Annual Report or the Annual Statistical Review
- any information on record to any other law enforcement agency provided the release of that information does not contravene any statute, is not confidential and is not likely to compromise any investigation
- any document to the court that is deemed necessary for undertaking an effective prosecution and is not considered to contain privileged information or is the subject of a court summons or subpoena
- any information that a defendant or legal representative would normally be entitled to access in connection with any court proceedings

For Polaris to be developed, a number of problems had to be addressed: a new network had to be developed; a new data server had to be found; relational databases had to be chosen; a new applications environment had to be found; business needs had to be analysed; workstations had to be expanded; gateways into human resource systems and external organisations (such as the ABCI and the Department of Transport) had to be built, and so on. Many internal and external organisations were also consulted: metropolitan police were the major source of information (for the sake of convenience), but regional police and other specialist groups (such as the Brisbane City Watchhouse, Fingerprints section and the PIC) were also included in the consultative process. However, it was conceded that 'it took too long — we put in too many bells and whistles — we should have cut it to core business' (Senior Information Technology Manager, Interview #13).

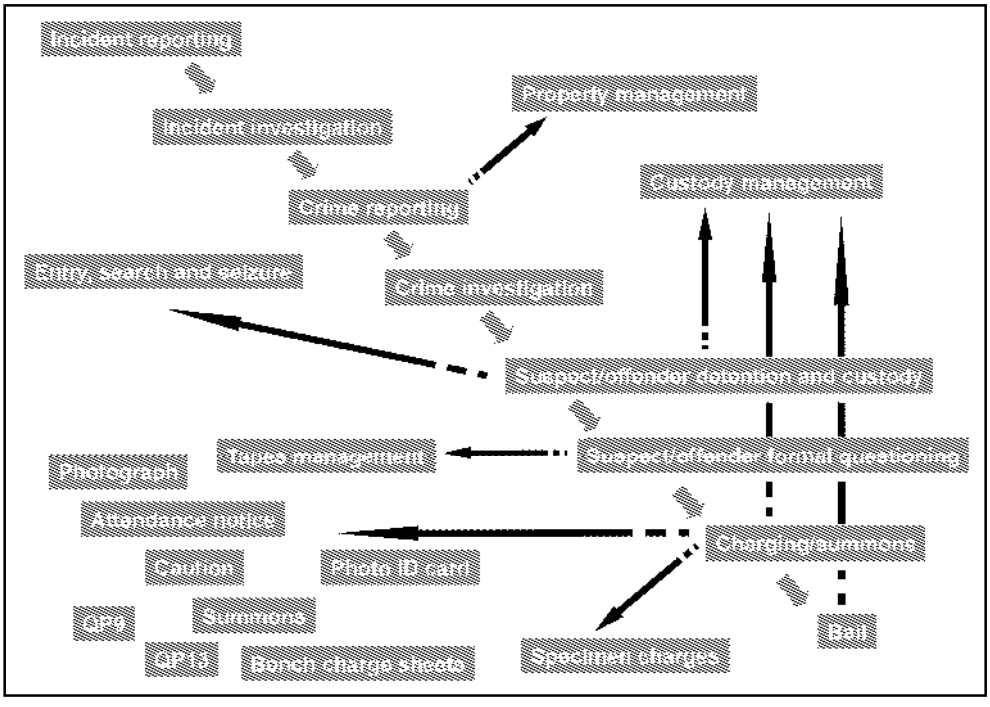
Overall, Polaris appears to have been hampered by technical complexity and funding insecurity — only half of the $10 million committed by the previous government was allocated by the incoming government for 1996–97 and the police had to continue to develop the system in-house rather than have the final stages developed externally by experts in the field. This has led to many officers expressing frustration that progress has been slow and not responsive enough to police concerns (Mortimer 1998). Some of these concerns are described further in chapters 5 and 6 of this report. It has also led to frustration on the part of the designers of the system. One of the concerns is that, by necessity, the system had to be developed and implemented in stages, but in the intervening time technology has changed. This creates 'a quandary — how do we change the technology when we're still trying to build on what we've already got?' (QPS Administrator, Interviewee #15).

Nevertheless, Polaris represents the largest modification to existing police computer systems that the Service has ever undertaken. It aims to provide:

- a system that is easy to use
- accurate and comprehensive information
- greater flexibility in searching for information
- a system that requires the 'once only' entry of a piece of information
- a system that allows access to all available information in the required topic with just one query.

Polaris has been, and will continue to be, introduced progressively through a number of releases. The three major phases of the release of Polaris have been designed to reflect the policing process. Figure 4.1 (next page) depicts the policing process (each stage requires data to be either entered onto or extracted from an information source before progressing to the next step), while table 4.1 (next page) identifies the links between this process and the release of Polaris.

Figure 4.1
The policing process



Source: QPS Interview #13: Powerpoint presentation on Polaris.

Table 4.1
Police processes and Polaris capabilities

Police processes	Polaris
Incident reporting Incident investigation Crime reporting Crime investigation	Polaris I: Warrants, drivers' licences, drivers' histories and national links (such as NEPI)
Suspects/offenders detention and custody Suspects/offenders formal questioning	Polaris II: Charging, offenders, criminal histories and vehicles
Charging/summons Bail Court results/offenders' histories[a]	Polaris III: Arrest and custody, seized property and exhibits

Note

a The Courts Modernisation Project is being conducted by the Department of Justice. When this is complete all courthouses and prosecutions will receive the Bench Charge Sheets electronically.

Other current systems

The major IT systems in the QPS can now be grouped into the following categories:

1. **A crime reporting system.** CRISP records all reports of suspected or actual crime. Entries are required only for indictable offences (e.g. homicide or assault) or simple offences of a serious nature (such as unlawful use of a motor vehicle, unlawful possession of property and offences under the *Vagrants, Gaming and Other Offences Act 1931*).
2. **Incident-based systems for command, control and dispatch.** CAD operates within the metropolitan area and some of the larger provincial areas, and the Incident Management System (IMS) operates in some rural and suburban areas. When a call is received from the public, the information is recorded by the police communication centre on either the CAD or IMS systems and is radioed to an available patrol unit for action. The systems record information about the call such as the nature of the offence, the name of the informant, the location of the problem and the times that the patrol car acknowledges the call, arrives and leaves the scene.
3. **Internal communications services** such as e-mail and the Bulletin Board (Phoenix). All legislation is now recorded on the Bulletin Board for ready access to up-to-date information by police.
4. Various **indexes** (such as domestic violence, weapons, tattoos), many of which relate to legislative requirements (see 'Accountability Requirements', page 28).
5. **Traffic systems** such as traffic incidents (TIRS) and transport data (TRAILS).
6. **Intelligence systems** such as QUID and ARI.
7. **Other systems**, including daily activity logs of operational police; databases of persons, vehicles and vessels of interest; various forms packages (such as court briefs); human resources, financial and library management systems, electronic warrants and mobile data (MINDA and Maverick); and a variety of national linkages (such as NEPI and ACID).

The appendix describes the major IT projects implemented between 1994 and 2000.

Future directions

The QPS Information Management Strategic Plan for 1999–2001 (QPS, undated [a]), which integrates policing targets and information technology infrastructure and support, is outlined in table 4.2 (next page). Among other things, future developments will include:

- progressive updates to Polaris to the year 2004
- electronic access to CRISP by Polaris

Table 4.2
Information Management Strategic Plan, 1999–2001

Program	Corporate output area	Description
Decision Support Services	Proactive, problem-oriented policing (POP)	POP is a systematic and targeted approach to analysing and addressing crime trends and associated community problems that requires a broad range of information (CRISP, calls for services, crime and traffic accident reports as well as data from other statistical sources).
Crime	Crime detection, investigation and prosecution	In collaboration with the Departments of Justice and Transport at a State level, the ABCI and the NEPI (as part of the broader Commonwealth Government Crim Trac), the plan will provide support for: ▪ crime detection, investigation and prosecution ▪ combating organised and major crime ▪ ethical standards and public accountability. The QPS will also be standardising the ABCI system ACID and the Violent Crime Linkage Analysis System (ViClass), and is a major participant of the Criminal Justice Information Integration Strategy (CJIIS) to have interchange of Bench Charge Sheets and Court Outcome details.
Incident management	Preservation of public safety	A new incident management system will be introduced to handle major events such as the Olympic Games. A study is also to be undertaken on how to improve calls for service, which include emergency calls.
Traffic	Traffic policing, speed management and camera operations	Further enhancements to the traffic camera system, the wider use of information from the IMS and the implementation of a traffic complaints system.
Corporate services	Corporate services	The acquisition of a new Corporate Records Management System is under way to enhance administration of corporate records.

- desktop replacement whereby all Apple® class machines will be replaced with computers running the Windows 2000® operating system (there will be a transition period of two years wherein both systems will be running)
- an increase in the computer-to-person ratio
- a central forms service
- improvements to mobile data such as an improved capacity to access CAD and existing systems and applications now available only by direct 'in-house' access; mapping of Automatic Vehicle Location (AVL) and Officer Down notification capability; automatic update of the QPS Activity Report Index (ARI); an ability to generate patrol logs, direct capture of property seizures, NTAs, Search Register and detaining information as required under police

powers legislation, the ability to record and print statements at the scene; and e-mail and Bulletin Board availability.

Managing the development of information technology

Information Management Division

As discussed, the IMD was established in 1993 as a result of the PSMC Review of the QPS. The Division has responsibility for the provision of a range of services including information planning, information systems development and implementation, the provision of police information, management of corporate databases and an information resource facility that incorporates statistics, data entry, library facilities and crime information such as warrants and criminal histories.

Within the IMD, there are several centres and branches with differing responsibilities:

- *Information Systems Branch* (ISB). The branch is responsible for the development and operation of corporate computer systems and its associated infrastructure. This is achieved through four primary services:
  - — Applications Section, which is responsible for the design, construction and maintenance of the programs that make up the IT systems.
  - — Systems Integration, which manages the computer databases and ensures IT systems effectively interoperate. This section is also responsible for information standards coordination.
  - — Technical Infrastructure Section, which provides processing storage and data networks that link to desktop computers throughout the Service.
  - — Operations and Administration, which reviews operational performances, provides change management processes and manages the impact of changes on the systems users.
- *Information Resource Centre* (IRC), which is responsible for statistical services, expert services, virtual library services (on the Bulletin Board), geographical information services and Web management.
- *Information Planning Branch* (IPB), which is responsible for information strategic planning, information operational planning and evaluation of information services, the Information Steering Committee (ISC), total cost of ownership end-user survey, project reports and ISC reports.
- *Information Security Section* (ISS), which is responsible for access to and investigation of information systems use, information security auditing, information security policy development, roles and responsibilities, security awareness training and awareness (video and handbook), contact number,

e-mail systems administration (internal and external), and the issue of user-IDs and passwords to authorised users for the QPS mainframe, Polaris, TRAILS, EAGLE, NEPI and QPS computer terminals.

- *Police Information Centre* (PIC), which is responsible for the development, preparation and implementation of information policy, procedures and legislation including CRISP, Polaris, Warrants and Polaris offender histories, negotiation with other agencies, the Information Service Centre, Information Support Unit, Warrant Bureau, Crime Management and Offender Management.

Planning processes

Within the IMD, there are planning processes that address the short-term tactical requirements of operational support by way of existing systems and services as well as the longer-term strategic requirements for the delivery of a whole new range of systems and services. To ensure that the IT systems suit operational police, the ISB convenes a working party for each module of every system to be developed or modified. The usual procedure is as follows: stakeholder analysis is carried out to see who the changes will affect the most; consultation is undertaken statewide; a prototype is developed; benchmarking procedures are undertaken; and policies and procedures are altered accordingly (Information Technology Manager, Interview #5). But there are mixed feelings about the effectiveness of these procedures — one IT manager suggesting that:

> … it has tended to be that the information technology has driven the policing rather than the police driving information technology … [the police] should be having a bigger input and making sure that they get what they want … Police are in a position … to make information technology work for them, they call the shots, they make the decisions and the Executive are in the position to say 'this is what we require, this is what we need, make it happen'. (Interview #9)

Formal documents, such as the Information Strategic and Infrastructure Plan,[10] the Information Technology Operational Plan, The Corporate Data Model[11] and the Corporate Systems Architecture,[12] have been developed to provide documentary support for the planning process (QPS 1995). Change Management Procedures also apply to all computer systems and platforms that are administered, operated or

10 According to the QPS Information Strategic Plan (1995–2000, p. 3) achieving a more effective police service is intrinsically linked to information management. Success in meeting the fundamental objectives of the Police Service hinges on having accurate and timely information available to all police.

11 The Corporate Data Model forms the basis for the policies and standards upon which all QPS information will be specified and standardised before implementation in a computer database.

12 The Corporate Systems Architecture concentrates on hardware issues and outlines how the technology needs to be arranged to support the Information Strategic Plan.

project-managed by IMD. Only authorised and licensed software that has been purchased and supported by the QPS can be installed on QPS computers, and all changes to any element of any system must strictly adhere to the QPS Change Management Procedures.

Before 1999, a number of 'bootleg' or 'rogue' information technology systems were developed by motivated QPS staff to fill a gap or perceived lack of appropriate IT support at corporate level. In an effort to overcome this the Information Planning Branch endorsed the Information Systems Project Initiation Framework in 1999, which provides an overall management structure to establish, redefine or dispose of information systems project proposals (QPS Bulletin Board, 2001). The framework is underpinned by a series of gates:

- *Gate 1* provides an initial assessment of the proposal to ensure adherence to QPS goals.
- *Gate 2* stops ad hoc projects from commencing. All proposals must receive ISC approval for an initial investigation.
- *Gate 3* provides a check to ensure that the proposal stays within the defined guidelines and goals, that funding is allocated and that the most appropriate course of action is taken.
- *Gate 4* provides a final check before implementation to ensure that the most appropriate methods have been chosen and that a project board overseeing the proposal has been established.

The underlying concept is for projects to be initially characterised according to their strategic priority and corporate impact. The following classification system is used:

- *Corporate:* A statewide information system employed by all regions, divisions and commands.
- *Regional:* An information system used by a few regions or divisions only.
- *Local:* An information system used at a branch or district level only.
- *Broad:* Used by the majority of police and/or staff in the defined area.
- *Narrow:* Used by a limited number of police and/or staff in the defined area.

Internal review

Since 1996, IMD has conducted an annual client survey of operational police and executive management to inform the ISC of the Service's progress on the Information Strategic Plan, and to identify management information that should be monitored. The survey supports the strategy proposed by the 1995–2000 Information Strategic and Infrastructure Plan to monitor and review information management performance.

Over the years, the survey results have highlighted a number of improvements. They have also pointed to considerable difficulties that do not appear to have been resolved. Selected results of these surveys are referred to in this and subsequent chapters.

Other information management processes

Apart from the IMD, there are a number of other internal groups at the QPS that oversee the role of information management. There are also a number of internal restrictions (such as information security, data quality, training requirements and staff turnover) and external pressures (such as legislative and watchdog requirements and external data requests) that exert considerable pressure on the types of IT systems that are chosen and the ways in which they are implemented. The external pressures have already been discussed. This section discusses the internal restrictions.

Management

These internal groups include:

- The *Information Steering Committee* (ISC) chaired by the Commissioner of Police (COP), which coordinates the management and application of the information resource of the agency (Department of Communication and Information, Local Government and Planning, Qld, Information Standard 16, 1999b). The ISC meets every three months and has responsibility and accountability for ensuring that:
  - — the use and application of the agency's information resource are consistent with the corporate directions and business functions of both the government as a whole and the agency as a single entity
  - — the agency's deployment of information technology is directed at the effective and efficient management of the agency's information resource
  - — appropriate security measures are developed, endorsed, instituted and monitored.
- The *Internal Audit Branch of the Ethical Standards Command (ESC)*, which provides senior management with a professional consultancy service and, among other things, the Audit Plan for the Year 2000, which includes a review of quality assurance in the IT environment.
- The *Risk Management Committee*, established to perform tasks required by government departments and agencies as specified in the *Financial Management Standard 1997,* ensures that management accountability is supported by proper systems and controls, and ensures that there are systems to collect data that will enable the committee to monitor the effectiveness of risk management.

- The *Inspectorate and Evaluation Branch*, which provides an independent assessment of management functions by implementing performance measures, inspections, internal audits, research and evaluation and information audits throughout the QPS with a view to improving performance, accountability and integrity.
- Each region also has the support of a *Regional Information Management Officer* (RIMO) and, in some instances, several technical assistants who support them. According to focus-group participants, however, the distribution of these officers is dependent upon the support and enthusiasm of the Assistant Commissioner in each region. The RIMOs in our focus group reported having little to do with IMD, although they would prefer IMD to play a greater role in their coordination across the State. Rather, they report directly to the Assistant Commissioner in their region and service the information technology needs of the police in their area. This can include development and integration of computer software (including corporate and rogue systems), coordination of provision of training for new corporate systems, provision of local out-of-hours help-desk facilities and participation in a number of local management decisions such as budget and risk management, and the local application of statewide information technology concerns such as Year 2000 compliance and the Olympic Games. Their role appears to include the qualities of management and service provision. Since the research for this report was undertaken, another, more senior role has been developed — that of *Regional Information Resource Manager* (RIRM). We believe that ten new positions have been created — one per region or command.

Information security

The need for information security affects the development and implementation of all QPS information technology systems. The *Financial Management Standard 1997* states that each information system must provide for:

- controlling access to the system, including, for example, physical controls on access to computers and use of passwords to restrict access to authorised purposes only
- maintaining an adequate audit trail
- obtaining approval before developing or changing the agency's software applications
- implementing, operating, maintaining and securing the information system
- specifying, developing, modifying or purchasing information systems for the agency's business needs
- recovering the information system if there is a system breakdown.

As discussed previously, the ISS of the IMD is responsible for the guidance and authority of information security activities within the QPS (information security is also monitored internally by the ESC and externally by the CJC). ISS provides direction, technical expertise, awareness training and advice to ensure that Service information is properly protected. However, in response to the question '[do] you think [that] the procedures at the moment are adequate', one interviewee commented that 'no, I don't believe security in any government department is adequate, and that's my very honest opinion' (Senior Information Technology Manager, Interview #9). The interviewee went on to state that the greatest threat is internal — 'the unauthorised release of information … it's very difficult to control because if you need access to certain information to do your job then you have to be trusted to take that information and use it under what the procedures and guidelines say … with 12 000 users it's very difficult to monitor every person, every day … to ensure that they're not doing something that is incorrect or outside the law'. A QPS Administrator (Interview #15) also indicated that, despite a promise in 1993 to implement the National Police Research Unit Standards of 'highly protected', 'protected', 'in confidence' and 'unclassified' material, these standards had not yet been implemented. This issue also attracted the attention of the CJC in a recent investigation — see *Protecting Confidential Information*, CJC 2000b — and these standards are now currently being implemented across the State.

There are several ways in which information security requirements affect police and civilian staff:

- Comprehensive training on information security must be undertaken by police and civilians. The Police Recruit Operational Vocational Education Program (PROVE), the Police Operational Conversion Course (POCC), the First Year Constable (FYC) Program and the Investigations and Intelligence Training Program (IITP) provide training for police. Civilian staff 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.
- All QPS and Polaris users must change their password every 90 days. Access and privilege management is dependent on the role of the user. Currently there are 10 500 users with access rights to Polaris, and 11 500 to the QPS system (CJC 2000b).
- All official user activity is recorded. Audit trails are able to record details such as dates, times, userids, terminal IDs and transactions, and can be retrieved at any time. In the case of Polaris, the keystrokes of a user can be played back in real time. Audit trails were monitored at random between 1994 and 1996 by the ISS, but this practice has been discontinued, despite the Service having the facility to do so (CJC 2000b). However, about 400 requests to search audit trails

are processed each year — these requests come from the CJC, the ESC and commissioned officers within the Service. About 40 per cent of these requests are related to the misuse of information; the rest are used to verify the work undertaken by operational police for court presentations.

Data quality

Raw data collected and stored by the IRC are audited every two years by the Australian Bureau of Statistics (ABS). However, an information technology manager suggested that the quality of the data needs to be 'tightened up before it can be used' (Senior Information Technology Manager, Interview #10). The issue of data quality is addressed in chapters 4 and 5.

Training requirements

It is compulsory for police to undergo procedural training in relation to new systems. Each police officer is allocated two days per month for overall training. This allocation includes all aspects of policing (such as new legislation), not just training related to information technology.

Most training is provided by self-paced CBTs, which are available on the Bulletin Board. This form of training provides a much cheaper option (at about $0.5 m) than the face-to-face 'train the trainer' programs (about $3 m) that were used for the implementation of, for example, the Criminal Code. (Senior Information Technology Manager, Interview #12).

The former Expert Support Unit was responsible for education in the use of advanced information systems, including specialised computer training and operational support across the State. The unit provided training and ongoing support to investigators, intelligence officers, OICs, Neighbourhood Watch Officers, crime managers and tacticians in CRISP, Indepol templates, CRISP Macro lists and Free Format Inquiries, crime statistics, MapInfo, NEPI and the Bulletin Board. It also designed training packages for use with recruits at the Academy, but involved the Academy 'heavily when preparing the training documentation so that it suits their needs' (Information Technology Manager, Interview #5). According to one interviewee, in the early 90s:

> [there] really wasn't any training given at the Academy, even in computer systems — we could never get it on the curriculum — always the response was there's no room for it in the curriculum, we're too busy telling them about the law and operational stuff. So we never got any of the information stuff into the Academy … and we never got it into the senior officer training programs — there was none of it in there. (Senior Information Technology Manager, Interview #12)

The Unit is now called the Expert Services Section, and its current role is to extract and analyse data and develop innovative technological solutions for contemporary policing issues. The training role has now been transferred to the Academy. The Police Education Management Education Unit at the Academy has a requirement to:

- deliver the Initial Service Computing Course to those personnel undertaking initial service training
- deliver modules of the Initial Service Computing Course to other courses as appropriate
- provide training to police and staff members in the use of Service computer resources
- develop courses and training resources.

The QPS also provides Regional Education and Training Officers and District Education and Training Officers (RETOs and DETOs) and Regional Education and Training Coordinators (RETCs), who oversee the training within their own areas.

Problems with training (particularly for Polaris and CRISP) were raised by many research participants. As one senior information technology manager said, 'there was never enough money to do training properly' (Interview #12). Other issues such as inadequate coverage, poor timing and lack of access were also raised. These are discussed in greater detail in chapters 4 and 5 of this report.

Information technology staff turnover

A number of research participants pointed out that the relatively poor salary levels for information technology staff within the QPS meant that staff turnover was rapid and that valuable information and corporate knowledge were consequently lost. This has been exacerbated by the withdrawal of government funding, as one senior police executive observed:

> [The] best laid plans and operational plans can get fouled up by politicians — particularly when you have a change in government and a change of priority … We had a commitment of $30 million for information technology development over three years, 10 million a year … We were about to get the first instalment of the second three-year 10 [million], when we had a change in government and they … cut the 10 million in half … This meant all the projects, particularly Polaris … had to be pruned to meet a $5 million budget … We started to build up a fairly good reservoir of specialists … and when it was cut in half we had to let some of them go … not only did we lose the individual but we lost the expertise … (Senior Police Officer, Interviewee #4)

The current turnover figures are unknown, but according to a participant who was reinterviewed shortly before publication (Senior Information Technology Manager, Interviewee #10) staff turnover has slowed considerably and is not the problem now that it once was.

Summary

This chapter has described the developments and changes in the extent and sophistication of information technology services for police in Queensland within the last decade. These developments were partly driven by technological advances that overcame deficiencies in earlier systems and partly by external demands for data and accountability. The transition from humble beginnings to the availability of different types of computer systems and applications for daily use by police is impressive. While the QPS has attracted considerable criticism for its management of information technology, it has been under tremendous internal and external pressure to provide a state-of-the-art system that: satisfies legislative and watchdog requirements; is transparent for accountability and auditing purposes; provides accurate and up-to-date statistics to external and internal user groups; and provides an ongoing tool for the day-to-day use of operational police, along with systems capable of superior manipulation for intelligence analysis. However, because successive governments have tended to assign a higher priority to funding capital works and police numbers, the large and growing demand for information technology services has not been matched by the levels of funding needed to achieve it. Funding for such endeavours has been limited and sporadic.

The following chapters will illustrate how information technology has been used in the QPS, the problems and difficulties encountered, and its impact on policing.

Chapter 5:
Impact of IT on police work

As discussed in chapter 2, a major imperative for police organisations to invest in information technology is to take advantage of technological advances to improve effectiveness and efficiency. Has information technology achieved this goal in the QPS? In this chapter we examine the impact of information technology on police work and the quality of service to the public.

General impressions

When we asked respondents in the survey whether information technology had made any difference to police work, the majority (72%) thought that it has made 'a great difference', about one-quarter (26%) thought it has made 'a little difference', while a minority (2%) thought it has made no difference at all.

When these perceptions were broken down by respondent characteristics, it became clear that those who have had longer service in the QPS and those in higher ranks were more likely to indicate that information technology has made 'a great difference' to police work (chi-square, $p < 0.05$). In fact, 9 out of 10 respondents with more than 20 years of service in the QPS (table 5.1) and 9 out of 10 respondents at the rank of inspector held this view (table 5.2). This is consistent with the findings in the focus-group discussions, where longer-serving officers often described in lively detail how cumbersome the old technology was:

> I remember the arrival of the first computer at the information bureau to check stolen cars. WOW! That was about '76 or so … [people were] excited. Instead of radioing in from a car and have someone go away and check microfiche and tickertape … We're talking about building to building, someone using tickertape going somewhere else and someone else then going and looking at microfiche. Then you get a tickertape answer back down the system. Then they brought the answer out on a card, stick it in a vacuum tube suction transfer

Table 5.1
Difference information technology has made to police work by years of service in QPS

Information technology has made:	*Per cent of respondents by years of service*				
	5 years or less	**6–10 years**	**11–15 years**	**16–20 years**	**More than 20 years**
– a great difference (%)	66	75	79	79	89
– little or no difference (%)	34	25	21	21	11
Total respondents (*n*)	216	77	32	58	45

Table 5.2
Difference information technology has made to police work by rank

Information technology has made:	*Per cent of respondents by rank*					
	First Year Constable	**Constable**	**Senior Constable**	**Sergeant**	**Senior Sergeant**	**Inspector**
– a great difference (%)	**69**	**63**	76	85	83	94
– little or no difference (%)	**31**	**37**	24	15	17	6
Total respondents (*n*)	**123**	**123**	78	62	36	16

> device — it would go 'whiit' through the building, come out at the radio operator. He'd read it back, and hopefully you're still in radio contact with an old radio that you used to have to switch off so that it didn't overheat. And then you'd get the message back, and then there may have been a typo somewhere along the line, and they'd say, no, that's not what we said, could you check 1,2,3,4,5,6 not 1,2,3,4,5,7? And it goes through the whole process again. (FG9: Specialist Investigators)

Frequency of use

To assess the use of some of the major information systems such as CRISP, MINDA, TRAILS, Polaris, NEPI, indexes and intelligence databases, we asked survey respondents how often they used these systems, providing them with the answer options of every day, several times per week, once or twice a week, very rarely and never.

As table 5.3 (next page) illustrates, just over half of all respondents reported using CRISP (64%), TRAILS (51%), Polaris (62%) and the indexes (51%) every day. Rank, however, appears to play a significant role in information technology use, with the lower ranks of FYC and Constable much more likely to report using CRISP, TRAILS, Polaris and the indexes on a daily basis than officers in the more senior ranks —

Table 5.3

Information technology system use by rank (per cent of all survey respondents)

Rank	How often use system	Per cent of respondents by system: CRISP (n = 457)	MINDA (n = 419)	TRAILS (n = 448)	Polaris (n = 456)	NEPI (n = 447)	Indexes (n = 444)	Intel databases (n = 448)
All ranks	Every day	64	4	51	62	9	51	17
	Several times a week	17	8	25	22	17	29	24
	Once or twice a week	7	5	9	6	21	8	19
	Very rarely	11	27	8	8	35	10	23
	Never	2	57	6	3	18	3	17
First Year Constable	Every day	84	3	65	80	11	67	27
	Several times a week	15	18	26	19	21	32	33
	Once or twice a week	<2	11	4	<2	21	<2	23
	Very rarely	0	30	4	0	40	0	16
	Never	0	38	<2	0	8	0	<2
Constable	Every day	77	3	64	76	11	62	17
	Several times a week	16	6	26	20	19	26	33
	Once or twice a week	5	3	8	2	28	8	18
	Very rarely	<2	35	0	<2	36	4	23
	Never	0	53	2	<2	6	<2	9
Senior Constable	Every day	49	4	46	53	8	41	15
	Several times a week	23	0	33	30	21	33	17
	Once or twice a week	15	4	6	8	23	13	17
	Very rarely	13	23	9	8	30	12	29
	Never	<2	69	6	3	19	<2	23
Sergeant	Every day	47	6	37	45	7	33	7
	Several times a week	18	0	27	31	17	29	9
	Once or twice a week	8	<2	15	10	22	14	19
	Very rarely	23	15	14	11	25	19	29
	Never	5	78	7	3	30	5	36
Senior Sergeant	Every day	14	0	3	8	3	14	3
	Several times a week	28	0	26	28	11	29	8
	Once or twice a week	6	3	17	22	6	9	8
	Very rarely	44	16	31	36	40	40	33
	Never	8	81	23	6	40	9	47
Inspector	Every day	6	0	0	0	0	13	0
	Several times a week	0	0	0	0	0	7	0
	Once or twice a week	25	7	31	13	13	27	13
	Very rarely	44	0	31	60	38	33	25
	Never	25	93	38	27	50	20	63

indeed, inspectors mostly reported using these systems only once or twice a week, very rarely or never. On the other hand, few officers in any level reported daily use of MINDA (4%), NEPI (9%) or the intelligence databases such as the QUID and ARIs (17%), again reflecting operational and specialist requirements.

Time use

If one of the advantages of using computers for information processing is speed, then police officers should find that information technology would enable them to spend less time on tasks such as reporting ('paperwork') and free them to do crime-related tasks such as patrolling the streets and responding to citizens' calls for service. Evidence from this research suggests, however, that this has not been the case.

Table 5.4 shows the responses to the survey question, 'has information technology changed the way you use your time?'. About half of the respondents did not think that information technology had made any difference to the way they used their time. However, a fairly substantial proportion thought that, as a result of information

Table 5.4
Perceived impact of information technology on time use

		Per cent of respondents		
Time spent on …	***n*[a]**	**Less time spent**	**About the same time spent**	**More time spent**
… satisfying accountability requirements.	459	10	49	41
… paperwork (preparing reports).	470	19	45	36
… planning, organising or analysing information.	413	16	54	30
… supervising or checking work of staff.	343	15	59	26
… preparing court briefs.	407	28	49	23
… responding to demands from staff.	370	14	67	19
… investigation of crime or gathering of evidence.	421	21	61	18
… patrolling the streets.	389	39	45	16
… informing citizens on the progress of their case.	410	25	64	11
… interacting with members of the community (not related to crime or emergency).	408	30	60	10
… responding to calls from citizens.	400	20	70	10

Note
a Excludes respondents who indicated 'not applicable — this is not part of my job'.

technology, they spent more time satisfying accountability requirements (41%); doing paperwork (36%); planning, organising or analysing information (30%); and supervising or checking the work of staff (26%). In addition, a sizeable proportion indicated that they spent less time patrolling the streets (39%); interacting with members of the community in non-crime or non-emergency situations (30%); informing citizens on the progress of their case (25%); and responding to calls from citizens (20%). The perceived impact of information technology on time use for the other items listed in the questionnaire was less pronounced, with roughly the same proportion of respondents reporting 'more time spent' and 'less time spent'.

The perceived impact of information technology on time use is not uniform. Table 5.5 shows selected items on time use broken down by rank of respondent. Although all police are affected to some extent, it is clear that respondents in the higher ranks (Senior Constable and above) are more likely to report spending more time on accountability requirements, 'paperwork', planning, organising or analysing information, and on supervising or checking the work of staff as a consequence of information technology. They are also more likely to indicate that they spend less time patrolling the streets, interacting with the community and responding to calls from citizens, although these activities were often not part of the job for those in the upper ranks (Sergeant and above). Tests for significant differences could not be conducted on these latter items, due to a number of cells with small expected values, especially among the Inspectors (see table 5.5).

We asked survey respondents how much time they actually spent during their last shift filling out indexes, searching databases, reading and sending e-mails and reading the Bulletin Board. On average, about half an hour was spent on each activity during that shift:

- Indexes: 39 minutes
- Databases: 43 minutes
- E-mail: 34 minutes
- Bulletin Board: 21 minutes

Some statistically significant differences were detected by rank, with officers in the lower ranks more likely to spend time on indexes and senior officers more likely to spend time on e-mail and the Bulletin Board (the use of databases did not differ), reflecting, no doubt, their roles (see figure 5.1, page 52). Combining these activities, it would appear that officers spend an average of about 2 hours and 19 minutes per shift undertaking these four IT-based activities.

We also asked respondents to estimate the amount of time they spent during the last shift using information technology to perform a number of administrative tasks. Table 5.6 (page 52) documents those tasks and the average time spent on each by all

Table 5.5
Selected perceived time use impact items by rank of respondent

	Per cent of respondents by rank					
	First Year Constable	Constable	Senior Constable	Sergeant	Senior Sergeant	Inspector[a]
ACCOUNTABILITY REQUIREMENTS[c]						
Less time spent (%)	14	7	13	7	6	6
About the same time spent (%)	61	56	33	38	39	31
More time spent (%)	25	37	54	56	56	63
Total respondents[b] (*n*)	121	122	79	61	36	16
PAPERWORK[c]						
Less time spent (%)	16	21	19	24	22	6
About the same time spent (%)	57	51	33	36	22	38
More time spent (%)	27	28	48	40	56	56
Total respondents[b] (*n*)	124	127	81	62	36	16
PLANNING, ORGANISING OR ANALYSING INFORMATION[c]						
Less time spent (%)	18	13	16	22	20	6
About the same time spent (%)	69	65	47	35	37	19
More time spent (%)	13	22	38	43	43	75
Total respondents[b] (*n*)	97	107	77	60	35	16
SUPERVISING OR CHECKING WORK OF STAFF[c]						
Less time spent (%)	16	15	16	18	13	7
About the same time spent (%)	72	74	52	40	48	47
More time spent (%)	12	11	32	42	39	47
Total respondents[b] (*n*)	74	82	69	57	31	15
PATROLLING THE STREETS[d]						
Less time spent (%)	27	34	54	50	64	100
About the same time spent (%)	52	47	37	42	29	-
More time spent (%)	21	19	10	8	7	-
Total respondents[b] (*n*)	124	121	71	38	14	3
INTERACTING WITH COMMUNITY (NON-CRIME, NON-EMERGENCY)[d]						
Less time spent (%)	28	22	38	36	25	56
About the same time spent (%)	59	69	57	56	55	44
More time spent (%)	13	10	6	9	20	-
Total respondents[b] (*n*)	121	121	72	45	20	9
RESPONDING TO CALLS FROM CITIZENS[d]						
Less time spent (%)	16	13	25	30	23	40
About the same time spent (%)	69	78	64	66	69	60
More time spent (%)	16	9	11	5	8	-
Total respondents[b] (*n*)	122	123	72	44	13	5

Notes

a Note small number of respondents.

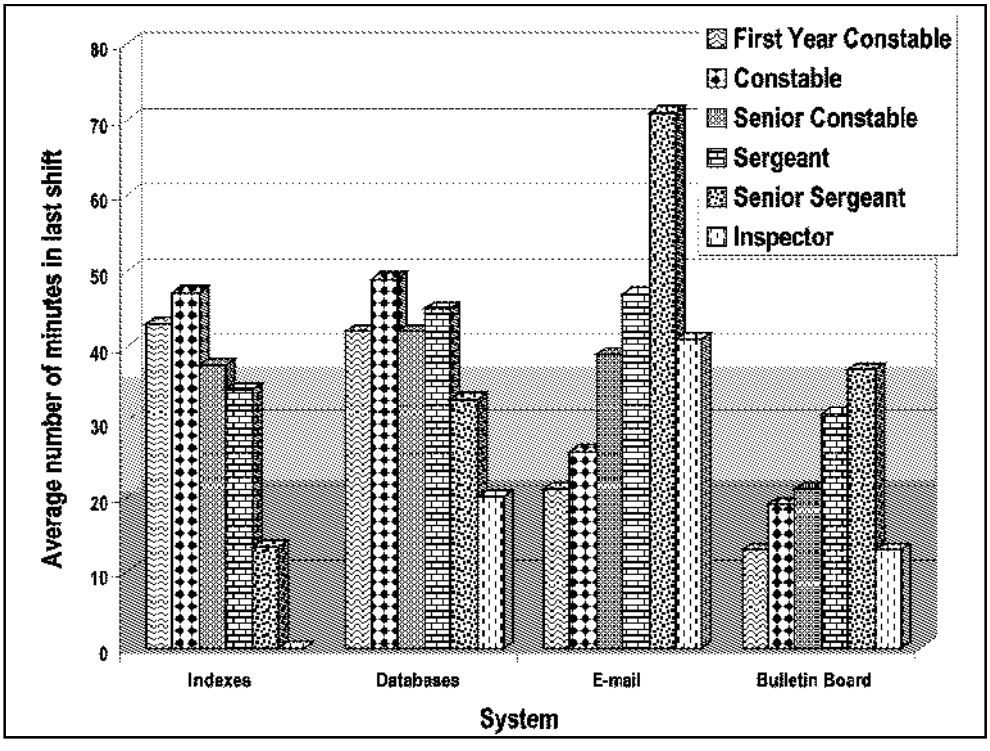
b Excludes respondents who indicated 'Not applicable — this is not part of my job'.

c Differences are statistically significant (chi-square, $p < 0.05$).

d Chi-square tests for significant differences could not be conducted since more than 20 per cent of cells had an expected frequency of <5.

Figure 5.1

Average time estimates, by rank, of respondents' use of different IT systems during last shift



Notes

Indexes	$p < 0.05$
Databases	not significant
E-mail	$p < 0.05$
Bulletin Board	$p < 0.05$

Table 5.6

Estimated average time spent using information technology on administrative tasks during the last shift (all survey respondents)

Task	Average time spent on task during last shift
Satisfying legislative or accountability requirements	22 minutes
Reporting on operational matters (e.g. incident or investigation progress reports, court briefs)	59 minutes
Communicating with other officers	50 minutes
Management or administrative purposes	34 minutes
Checking quality of information entered	11 minutes
Retrieving information for systematic analysis	10 minutes
Retrieving information for operational purposes	29 minutes

participants. Again, operational matters, such as incident and progress reports (59 minutes) and retrieving information for operational purposes (29 minutes) appear to take the most time, apart from communicating with other officers (50 minutes).

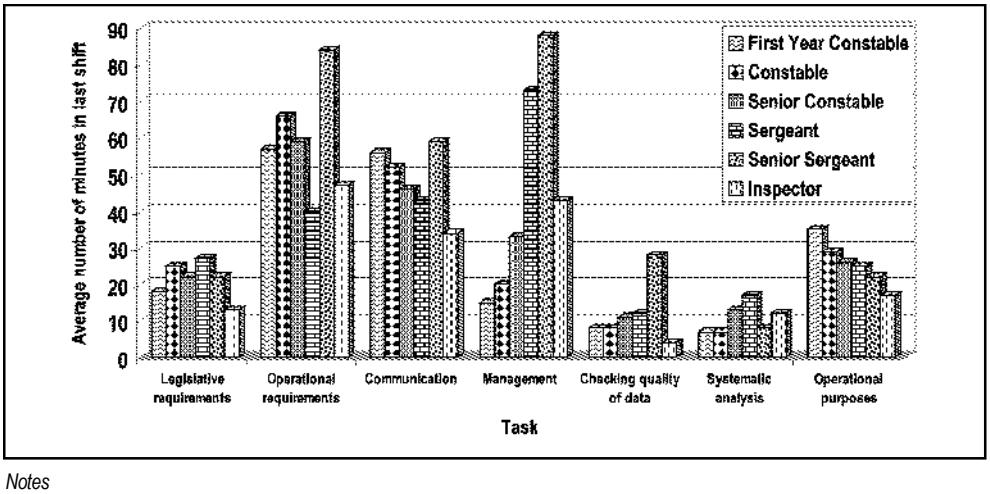
In total, respondents reported spending on average about 3 hours and 37 minutes per shift using information technology to undertake these administrative tasks. Again, however, some rank differences were noted: FYCs, Constables and Senior Constables were more likely to report using information technology systems for operational matters, while Senior Sergeants reported spending most of their IT time on management or administrative issues and communicating with others (see figure 5.2).

Many focus-group participants pointed out that police 'really can't do anything without a computer'. Time-use estimates provided by respondents suggest that police spent from 25 per cent to all of their time using information systems, depending on their role, the task at hand and the availability of computers.

The issue of police spending more time in front of computers and less time on the streets was often raised in the focus groups. As one frustrated general duties officer remarked:

> The basic thing is, you're out there to protect property and life and all that … we're out there in uniform to be policemen, we're not paid to be typists … A lot

Figure 5.2
Average time estimates, by rank, of respondents' use of IT for a variety of administrative tasks in last shift



Notes

Legislative requirements	not significant	Checking quality of data	p = 0.033
Operational requirements	not significant	Systematic analysis	not significant
Communication	not significant	Operational purposes	not significant
Management	p = 0.000		

> of shifts you will spend as much time behind the typewriter, or taking a CRISP report, or whatever, or on the phone to those village idiots down there, as you would be out locking a drongo up. (FG1: GDs)

Another participant of the same group said that 'technology has drawn a lot of people off the street and stuck them into offices'. Even though there were a lot of police 'on paper', very few are on the road. This concern was echoed by a participant in a focus group consisting of intelligence officers and tacticians:

> The operational police in this organisation as far as I'm concerned are still the core business … however, increasingly it is getting more and more difficult to get out on the road and do what we're supposed to be doing. It is time-consuming and the hierarchy in this Department right across the board need to understand that the job now is resource-intensive … that it takes longer to do things than it did before (FG5: Intel/Tacticians).

One IT manager told us that Polaris now allows managers to do such tasks as assessing how many warrants their staff have done per day or tracking the number of crime reports implemented and by whom (Interview #5). Clearly these would be time-consuming tasks. One crime manager who participated in the focus groups (FG5: Intel/Tacticians) illustrated this issue further — he reported having to assess at least 600 CRISP files per day to partially complete his daily tasks. Another OIC commented that:

> The systems aren't user-friendly to management … say, for instance, you want to do an audit on your master tapes for your station … in the current query field, you can't just type in XXX station as a division and go zap … that's what your master tapes are. You've got to go through each officer's registered number … and that's just ridiculous. (FG7: OICs)

Nature of work

Although there were a lot of complaints about technical problems connected with information technology among the focus groups, the survey results suggest that officers' assessments of the impact of information technology on their own work were generally positive.

Table 5.7 shows that the majority of respondents indicated that information technology has: allowed them to work more effectively (79%), made their work easier (66%), and helped them cope with the amount of information police need to do their work properly (59%). The gain in efficiency as a result of information technology was especially salient to police who had experienced the old technology. One participant in a focus group (FG9: Specialist Investigators) gave an example of 'how it used to be'. He said that, five to six years ago, to type a record of interview for a large

Table 5.7
Impact of information technology on individuals' work

Information technology has …	*n*	*Per cent of respondents* Strongly agree /agree	Neutral	Disagree/ strongly disagree
… allowed me to work more effectively.	480	79	19	3
… made my work easier.	479	66	26	7
… helped me cope with the amount of information police need to do their job properly.	479	59	31	10
… required me to follow unnecessary steps to get things done.	479	43	45	13
… made my work more interesting.	478	27	55	18
… taken some of the stress from my work.	479	25	44	31
… limited the amount of discretion I have.	479	25	59	17
… reduced the amount of paper used in my work.	479	19	24	57

investigation would take five to six hours. Now it could be done in half an hour from a taped record of interview.

Another dramatic example of improvement in efficiency and effectiveness was in the production and handling of court briefs, as pointed out by another focus-group participant. He said that, up to six years ago, briefs of evidence had to be produced using carbon paper in a typewriter, which meant that, if they made a mistake, they had to go back and retype it. With computers it is now easier to produce the briefs. Technology is at the stage where 'they can produce them on CD and take them to court'. It is now possible to show actual crime scenes in court. He said that the amount of work they have got now is 'astronomically more, better quality, more professional and we're achieving better results' (FG9: Specialist Investigators).

About a quarter (27%) of the survey respondents agreed that information technology has made their work more interesting, although 18 per cent disagreed, while 55 per cent neither agreed nor disagreed. One participant in an OIC focus group explained how information technology has made his work more interesting:

> I reckon it makes it a little bit more interesting in that you can search more for things. If you use your imagination a bit you can find a lot more information … If you're looking for Joe Blow again, then you can go in and search a lot more fields than just the basic ones and find out a lot more information, and you can

> come down at the end of the day and find out what their previous offences were, which will make you then look at it in a different way. (FG2: OICs)

On the negative side, a substantial proportion of the survey respondents thought that information technology had not reduced the amount of paper used in their work (57%), but has required police to follow unnecessary steps to get things done (43%). RIMOs who participated in a focus-group discussion gave numerous examples of how information technology has not decreased the use of paper among police. One story went as follows:

> I saw a novel one a couple of months ago — someone has a really big folder and any instruction or e-mail or report sent to him he has categorised into different sections, like CRISP or supervision. And anything he gets he puts into that, and he carries it in his bag with him in the car. So if he comes up against a situation he goes to 'lost kids' and he looks up exactly what the latest thing is he should be doing. Because often there are local instructions that his Senior Sergeant might have put out, or our Assistant Commissioner will have put out, it must be incredibly hard to remember all those things. (FG8: RIMOs)

RIMOs said that the biggest complaint they received was that when police print something from the Bulletin Board, it doesn't just print the page they want, 'so they don't actually read it on the screen; they've got to print it to read it and the older the person the more they have to print it to read it'. Others mentioned that administrative officers in some regions print out Bulletin Board information page by page and circulate it around the office in hard copy (FG8: RIMOs).

The feeling that police were required to follow unnecessary steps to get their work done was particularly strong among detectives, with 59 per cent agreeing and only 9 per cent disagreeing, compared with General Duties officers (40 per cent agreeing) and officers with 'other duties' (41% agreeing). These differences were statistically significant (chi-square, $p < 0.05$). Rank also mattered in respondents' perception that unnecessary steps had to be followed — percentages who agreed went up from 35 and 36 per cent among FYCs and Constables respectively to 51 per cent for Senior Constables, 53 per cent for Sergeants, 47 per cent for Senior Sergeants and 60 per cent for Inspectors (chi-square, $p < 0.05$).

Much of the focus-group discussions centred on the additional steps officers had to follow to get their work done. For example, one general duties officer explained that the old way of doing the QP9 (court brief) was to put it in the typewriter and wind it on, but it was quicker because you knew exactly where you wanted to go, there was no need to wait for each screen to come up. Another participant said that on the old system, it would take 10 to 20 minutes to complete a court brief, whereas now it takes two to three hours (FG1: GDs). This view was supported by officers from other focus groups:

> When I was at [name of station] years ago we could … do a RBT, pick up a drink driver, take him into town, process him, … have him charged, have a QP9 typed in the prosecutor's box, have all the paperwork done, be back on the road and the best we ever did it in was 40 minutes … That was on a manual typewriter. Now, … by the time everyone does all their compliance with their custody indexes and all their indexes and does everything else, finally gets through to CRISP to get a CRISP number, then they sit down in front of the computer to do the QP9 on the computer. And the QP9 on the computer takes a lot longer than the old manual typewriter. So I'm looking at hours. And so if an operational crew picks up a drink driver … by the time they get a breath operator, and just to get a CRISP number, without doing any typing, they'll be off the road a minimum of an hour and still then someone has to go back and type a QP9 somewhere within the next few days. Comments from the floor estimate that the process has gone from 40 minutes to 2 hours (FG6: GDs).

> You execute a search warrant under the PP&R [Police Powers and Responsibilities] Act for a drug matter, that's one computer entry for a start. You then do a search on the premises. You locate a quantity of drugs. OK, you've got your custody index for your person and you've got your drug index for that. You've got your property index for the exhibit, or your exhibit index. Your CRISP number. So you've got … I think it's about six as it stands at the moment, for drugs. (FG2: OICs)

In response to the statement 'information technology has limited the amount of discretion I have', about 25 per cent of survey respondents agreed, 17 per cent disagreed and 59 per cent were neutral. Further analysis showed that general duties officers were more likely to think that information technology has limited their discretion (27% agreed v. 14% disagreed), compared with detectives (19% v. 17%). Similarly, officers in lower ranks were more likely than those in higher ranks to agree: FYCs (26% agreed v. 14% disagreed), Constables (21% v. 16%), Senior Constables (26% v. 11%), Sergeants (32% v. 13%), Senior Sergeants (17% v. 31%), Inspectors (20% v. 40%).[13] The issue of discretion was raised in focus groups. One response was that it is a lot harder to write a file off because of insufficient evidence; a reason has to be entered for writing a file off. However, Constables can still find ways of cutting corners, as one participant explained in relation to whether a minor incident should be reported:

> The initiative there for the connie [Constable] is: Is this an insurance claim? Has he got my name? He doesn't know anything — and it's in the bin, because he lost a piece of garden hose. That's where the discretion is now, because the connies are cutting corners … The discretion there is: Is this going to be reported? This person has said it's not an insurance matter. This person doesn't want any feedback. There's no suspect nominated — in the bin! So they're cutting the corners there, risking being charged if this person comes back and

13 Differences are not significant (chi-square, $p < 0.05$) unless ranks are collapsed into fewer groups.

says to a Senior Sergeant on the counter one day, 'I reported this to Constable [X] and he said this' … (FG5: Intel/Tacticians)

Other police said that there are no shortcuts — the system was designed in such a way that it cannot be circumvented (FG4: Detectives). In fact, the system is capable of monitoring shortcuts: 'the shortcuts can now be assessed — if you are taking shortcuts, it can be seen that you are taking shortcuts' (FG5: Intel/Tacticians). Some officers felt that police had become rule-conscious to the extent that 'we get confused now if we can't find a rule about it' (FG5: Intel/Tacticians).

Although a quarter of the survey respondents agreed that information technology has taken some of the stress from their work, a marginally higher proportion (31%) disagreed. There was some interesting variation of this result by rank, with the highest proportion who disagreed among the middle ranks: FYCs (23%), Constables (20%), Senior Constables (48%), Sergeants (47%), Senior Sergeants (33%) and Inspectors (40%). Part of this was related to age, as further analysis showed that respondents aged 45 and above were most likely to disagree that information technology has taken stress from their work (46%), compared with the younger age groups: under 29 (21%), 30 to 44 (40%). These rank and age differences were both statistically significant (chi-square test, $p < 0.05$).

Quality and use of information

Table 5.8 summarises survey results in relation to the impact of information technology on the quality and use of information by police. A substantial majority of respondents agreed that information technology has led to an improvement in the quality of information (76%) but fewer felt the same way about the security of information (51%). A majority also thought that information technology has

Table 5.8
Impact of information technology on quality and use of information

		Per cent of respondents		
Information technology has led to …	***n***	**Strongly agree/ agree**	**Neutral**	**Disagree/ strongly disagree**
… improved quality of information.	468	76	21	3
… increased computer literacy among police.	463	75	20	5
… increased information sharing between police officers.	467	69	26	5
… improved security of information.	467	51	39	10
… information overload.	468	47	40	12

increased computer literacy among police (75%) as well as information sharing among police officers (69%). However, not everyone agreed that there has been an increase in information sharing. As one participant among a focus group of detectives said:

> A lot of information on the systems would be half of what people know, because people don't share their information. They don't want to share the information, because, if I've got some really good information about a group of baddies that I think I can get, there's no way I'm going to share it with these guys because I'm going to get the glory for it. And, and, I'll be able to get a promotion quicker than these guys because I've got a big job behind me. (FG4: Detectives)

Another participant in the group pointed out that information would not be entered into the system until an operation was completed because sharing that information might jeopardise the operation (FG4: Detectives).

A sizeable proportion of respondents (47%) indicated that information technology has led to information overload among police, but many were neutral about this (40%). This feeling of overload was particularly acute among more senior officers: for example, only 36 per cent of Constables agreed with this statement compared with 51 per cent of Senior Constables, 62 per cent of Sergeants and 69 per cent of Senior Sergeants and Inspectors. Similarly, older and more experienced respondents were more likely to suffer from information overload.[14] Sixty-eight per cent of those aged 45 and over agreed with this statement, compared with 53 per cent of 30–44 year olds and 38 per cent of those aged 29 and under. This issue was brought up by a participant in a focus group consisting of intelligence officers and tacticians. He said, 'I reckon half of us suffer from information overload', and there was general agreement from the group. He said he had a particular axe to grind in relation to the use of the Bulletin Board — 'there's so much going on it, it's overwhelming, and they can't keep up with it … if there was new legislation going out tomorrow, it would be on the Bulletin Board this afternoon and tomorrow morning we would be expected to know it' (FG5: Intel/Tacticians). Another participant observed:

> We seem to be information gatherers but not information disseminators, and a lot of our resources are going in to that, but I don't see a great deal coming back out … I think your research would show quite clearly that our figures, as far as what we're doing today, are essentially the same as what they were 10 years ago, but we're putting more into collecting the information (FG5: Intel/Tacticians).

E-mail was also said to be a major cause of information overload; some people struggled to deal with it, others coped by 'deleting everything' (FG8: RIMOs).

14 Statistically significant differences for rank and age (chi-square, $p < 0.05$).

Policing style and practice

To what extent has information technology changed the style and practice of policing in Queensland? Survey results (table 5.9) suggested that information technology has improved communication between police officers (70% agreed; 4% disagreed) and enhanced the professional status of police (53% agreed; 9% disagreed). According to 45 per cent of the respondents, information technology has led to police spending less time 'on the road'. As pointed out in the section on time use, almost 4 out of 10 respondents reported spending more time on 'paperwork' and satisfying accountability requirements. It is therefore not surprising that only 38 per cent agreed that information technology has led to a more problem-oriented police service (the rest were mostly neutral). Significant differences emerged for rank (chi-square, $p < .05$). Senior Constables (21%), Sergeants (19%) and Inspectors (19%) disagreed more often with the statement that information technology had led to a more problem-oriented police service than Senior Sergeants (11%), FYCs (6%) and Constables (2%).

The idea of smarter policing strategies was raised in one of the focus groups. Some officers mentioned the potential of 'intelligence-driven patrols', analysis of 'hot spots' and repeat offenders, and proactive crime investigations (FG9: Specialist Investigators). Others were more sceptical, 'who gets time for that?'. It was said that it doesn't happen — 'never will', although in theory it could happen. One focus-group participant explained the role conflict experienced by Intelligence Officers:

> Most of them are in regional offices. Most of their time is [spent] putting stats together for bosses. But that's not their role. Their role is to look at the crimes that are going on to target areas or offences. They don't have time to do it because they are collating crime stats for a management meeting. Because Intel officers aren't able to do their job, there's a whole bunch of baddies we can't get because they aren't looking at it. You might say we should do it, but where do we get time? We're task-orientated. [Intel officers] have to do *x* number of files

Table 5.9
Impact of information technology on policing style

		Per cent of respondents		
Information technology has led to …	***n***	**Strongly agree/ agree**	**Neutral**	**Disagree/ strongly disagree**
… improved communication between police officers.	468	70	25	4
… enhanced professional status of police.	463	53	38	9
… reduced police time on the road.	467	45	33	22
… a more problem-oriented police service.	468	38	52	10
… better proactive policing.	468	35	47	18

> in a month, and if they're not doing that, they're not getting *x* number of arrests, so they are tossed out of plain clothes. (FG4: Detectives)

Only 35 per cent agreed that information technology has led to better proactive policing, 47% were neutral and 18 per cent disagreed. There was some variation in this opinion by rank (chi-square, $p < 0.05$), with the highest level of agreement coming from the most junior and most senior ranks, as was the case with views regarding problem-oriented policing: FYCs (44%), Constables (38%), Senior Constables (25%), Sergeants (35%), Senior Sergeants (25%) and Inspectors (44%).

One area where information technology appears to have facilitated proactive policing in a dramatic way is the use of Maverick, a stand-alone computer used in police cars to check for outstanding traffic offence warrants based on vehicle or boat licence numbers, persons of interest and drivers' licences (see text box on pp. 63 and 64, 'Case study: The impact of information technology on police enforcement practices'). Focus-group participants were enthusiastic about Maverick, as a general duties officer explained:

> We use it [Maverick] all the time in regards to warrants and people wanted for questioning. And our clear-up rate in regards to crime and the number of warrants that we've executed … for the ratio of staff we have, is by far the best in South Brisbane and it's a fantastic system … It cuts down the number of times we have to use the radio, which frees it up for other cars. (FG6: GDs)

Another officer concurred, 'it's becoming more and more a necessary tool. When you get in a police car and it doesn't have one, you feel like you have lost something'. Officers with Maverick said that they do about 1000 checks a week (FG6: GDs).

Some officers were not entirely comfortable with the heavy reliance on information technology for information. As an OIC observed in a focus-group discussion, police no longer carry policing knowledge in their head:

> Troops on the road don't really have the time. They're out there and they're stuck with what they've got in their head. If they don't know it, they've got to ring up and ask somebody else. And then the supervisors … are digging into the system looking for them. We probably don't carry the knowledge base we used to carry … now on the Bulletin Board. Once everybody had their own set of Acts … and we don't have exams any more so that … training system is out where we covered everything. Now your training days tend to be specific. And once you come out of the Academy, if you don't know it then, you're really between a rock and a hard place. (FG2: OICs)

Reliance on information technology also meant the loss of 'local knowledge', as one general duties officer remarked:

> Information technology is good for number crunching, but you don't know the face. You can drive around for a whole shift and not see the same face twice.

Even 'number crunching', however, carries the danger that out-of-date information may be used to identify 'trouble spots'. (FG1: GDs)

Quality of service

Survey respondents were generally positive about the impact of information technology on the quality of police service. Six out of ten thought that information technology had led to improved police service to the public (62% agreed; 12% disagreed) and improved police response to crime (59% agreed; 12% disagreed). These opinions varied somewhat by rank, but not by location. Junior officers were more likely to agree that information technology has improved police service and response to crime than their seniors (see table 5.10). General duties officers were more likely to agree (65%) that information technology had improved police response to crime than detectives (55%) and officers in 'other duties' (47%) (chi-square, $p < 0.05$).

Focus-group participants provided some useful insights into how information technology had improved police service to the public. Several groups told us that CRISP had made a difference. As one OIC pointed out, with CRISP, police procedures are more transparent — the complainant can see the officer getting on the phone to file a report, 'now the public can see that something's really happening' (FG3: OICs). CRISP also allows victims and complainants to get faster feedback on the progress of their case by ringing up with a CRISP number (FG2: OICs; FG8: RIMOs). Police can also respond better to customer inquiries as they can access information about the

Table 5.10
Impact of information technology on police service by rank of respondent

	Per cent of respondents by rank					
	First Year Constable	Constable	Senior Constable	Sergeant	Senior Sergeant	Inspector[a]
IMPROVED POLICE SERVICE TO THE PUBLIC[b]						
Strongly agree/Agree (%)	72	69	54	50	53	56
Neutral (%)	21	28	25	31	36	19
Disagree/Strongly disagree (%)	7	3	21	19	11	25
Total respondents[b] (*n*)	127	125	81	62	36	16
IMPROVED POLICE RESPONSE TO CRIME[b]						
Strongly agree/Agree (%)	73	66	52	42	47	38
Neutral (%)	20	29	26	36	44	25
Disagree/Strongly disagree (%)	7	6	22	23	8	38
Total respondents[b] (*n*)	127	126	81	62	36	16

Notes
a Note small number of respondents.
b Differences are statistically significant (chi-square, $p < 0.05$).

Case study:

The impact of IT on police enforcement practices

One of the many recent technological developments in policing has been the introduction of mobile data systems that enable police to do various information retrieval tasks while on mobile patrol, such as conducting instant warrant and vehicle registration checks. The placement of computers in cars ('cyber-policing') is widely seen as one of the most important technological developments to occur in policing in recent years (Legosz and Brereton 2001).

In 1996 a few MINDA units were made available to the QPS by Queensland Transport free of charge. MINDA is a mobile, hand-held unit that communicates directly with a database at CITEC, which cross-matches information from Queensland Transport's TRAILS system (for details on vehicles, vessels and licences) and the QPS Polaris system (for persons of interest).

The unit enables initial checks on persons and vehicles to be made quickly. This is particularly valuable when a person or vehicle of interest has been detained due to the commission or suspicion of an offence, but can also provide valuable information on the existence of outstanding warrants, unregistered vehicles or unlicensed drivers during random checks on cars or persons (such as parked cars or pedestrians) while on patrol. For officers without such access, the car or person of interest often needs to have performed an illegal or suspicious action before a call will be placed to the communications operator to inquire about such details.

The database alerts the officer to the existence of a person, a vessel or a vehicle of interest, but the details (such as the offence to which the warrant refers and the amount owing) are not immediately available to the system user — the user must communicate by police radio with a communications operator who has direct access to the mainframe databases to obtain that information.

In the last few years MINDA has been superseded by a new system called Maverick (although some MINDA systems remain in use with general duties officers and other police who work primarily out of the office, such as water or mounted police and police working on beats). Maverick is a computer located in the boot of a police car (usually assigned to a traffic officer), which is accessed by a 'mini lap-top type' terminal inside the car. There have been several upgrades of Maverick that have been directly related to improved geographical access via the mobile network system. The latest version of Maverick (GSM), to be released in late 2001, will provide access to regional police, whereas the previous model (Mark II) was limited, predominantly, to police in south-east Queensland.

Currently there are about 120 Maverick units in use throughout the State. However, few officers have regular access to this technology — according to the survey respondents, only 4 per cent of 506 respondents reported using MINDA on a daily basis and 56 per cent reported having never used it. Compared to TRAILS, where 51 per cent reported using the system every day, and Polaris, where 62 per cent reported using the system every day, access by operational police appears to be quite limited.

Observations of MINDA and Maverick in operation were made for the study. The police whom we observed varied considerably in the extent to which they used the technology, ranging from one case study where police collected over $5000 worth of outstanding fines in the course of a few hours to another where the system was used for only a short time during the shift and produced no 'hits'. Factors that appeared to affect the level of use included how the patrol was tasked, levels of police interest in engaging in fine and traffic law enforcement, and the characteristics of the area being patrolled. However, while levels of use varied, we observed no resistance to the technology. To the contrary, the officers spoke favourably about this innovation and its ease of use.

Apart from fitting comfortably with the enforcement focus of policing, and helping to communicate a more 'professional' image to the general public, Maverick/MINDA has several practical features that

appeal to operational police. The system is easy to use and the operational benefits, in terms of ability to access information directly rather than going through a communications operator, are very tangible. In addition, police feel that they can control the technology, as it is basically up to them to decide whether or not to use it in a particular situation and they are not totally reliant on another person (the communications officer) to obtain the relevant information.

MINDA and Maverick have been two technological developments that have substantially improved police effectiveness in enforcing warrants.

The number of warrants of commitment executed by the QPS increased from around 3000 per month in late 1996 (just after electronic warrants were introduced as part of the Polaris initiative) to around 11 000 in late 1998, before dropping back to around 7000 in March 1999 (CJC 2000c). The upsurge in the latter part of 1998 corresponded with the clearance of processing backlogs, plus the introduction of database enhancements.

In most cases, warrants were cleared by the offender paying the outstanding fines on the spot (via the mobile EFTPOS facility) or at a police watchhouse. However, those offenders who would or could not pay were placed in custody — either in a police watchhouse or, if detention was for more than a few days, in prison. This increased enforcement activity contributed to an upsurge in the number of fine defaulters being admitted to prison — from around 80 per month in 1996–97 to over 200 per month in the latter part of 1998.

By 1998 'pure' fine defaulters accounted for more than one-third of admissions to Queensland prisons — up from around one-quarter in 1995. Because defaulters typically serve only short terms of imprisonment (an average of 19 days in 1997–98), they make up a much smaller proportion of the total prison population (around 8% in March 1999), but the high rate of turnover means that they are still a very significant administrative and financial impost on the prison system.

Although police became much more active in the enforcement of warrants in the latter part of the 1990s, as at 1 March 1999 there were still around 375 000 warrants for unpaid fines outstanding in Queensland, of which the great majority would have been traffic-related. Based on an average of five warrants per person, this represented around 75 000 fine defaulters (CJC 2000c). Given that around 5 per cent of fine defaulters apprehended by police were unable or unwilling to pay their fines, a sustained enforcement blitz would have had the potential to overwhelm the State's prison system.

In response to the growing problem presented by fine defaulters, in late 1999 the Queensland Government introduced the *State Penalties Enforcement Act 1999.* This legislation is aimed at reducing the use of imprisonment for fine defaulting, principally through the creation of a State Penalties Enforcement Register (SPER) empowered to pursue recovery of fines by a variety of means. It appears that this initiative has had an initial effect, with fine defaulters admitted to prison dropping by 13 per cent in 1999–2000 (CJC 2000c), although it is too early to tell whether this trend will be sustained.

While some corrective action has now been taken by the Government, this did not happen until the pressures on the State's prison system reached crisis point. These problems could have been avoided, or at least ameliorated, if SPER had been introduced before enhancing the technology for issuing and enforcing fines. However, when initiatives such as electronic transfer of warrants and MINDA and Maverick were being designed and implemented it seems that little thought was given to the possible consequences. From the point of view of the QPS and Queensland Transport, the emphasis was very much on achieving agency-specific efficiency gains and generating increased revenue. A compounding factor was the lack of an effective central coordination mechanism in the Queensland criminal justice system, which meant that there were no processes in place for evaluating the wider impact of proposals to adopt new technology or for synchronising changes to policy and organisation.

This case study provides a good example of how IT innovations can have substantial flow-on effects, especially when made at the front-end of a larger system. The case study also highlights the importance of having proper change management and coordination processes. The scale and nature of the impact of some information technology innovations may be impossible to predict in advance, but in other cases they are likely to be reasonably foreseeable. In the context of the criminal justice system, the challenge is to develop processes which ensure that policy makers focus on these issues at the outset, rather than reacting after the consequences have become apparent.

case and identify who to contact (FG5: Intel/Tacticians). Some participants noted the paradox that faster and more efficient service does not always result in customer satisfaction, a good example being the efficient collection of fines with the use of Maverick.

While there seemed to be agreement that information technology had improved police service at the level of customer interface, there was less consensus about the benefit of information technology in improving police response to crime. As one OIC pointed out in his/her focus group, police are not as directly involved with the public in criminal investigations as they were five to ten years ago, 'go to the computer, you retrieve off that what you need ... without actually going and knocking on doors … finding out "hey, what's Joe Blow been up to?"'. Even though intelligence is extremely good, these officers felt that it will never take the place of basic hands-on traditional intelligence gathering — getting out on the street, talking to people, finding out what's going on (FG2: OICs).

In another group there was a fair amount of dissatisfaction with the closing down of police stations. It was said that divisions are now so big that police don't get out of cars to talk to people. There are not enough cars to send out to people, and people won't come in to distant stations to report, but 'the department sees this as a reduced crime rate' — they closed down police stations because of this 'wonderful technology'. With the closure of local police stations (clustering), one officer said you could go to an area now and ask who their 'local grubs' are, who is doing the B&Es in the area, who are the drug dealers, and the police can't tell you. He said that if you ask local business people 'who's your local OIC?', they wouldn't know — they might see a police car once in a blue moon. It was claimed that police service is less personal than it used to be because of ideas such as clustering, which destroy local knowledge (FG1: GDs). Officers were sceptical of claims that crime rates had dropped, 'they use the excuse that technology is improving things so they can close police stations down'. They argued that the public are refusing to report crime because they are not getting the service (FG1: GDs).

Information technology has given police the potential for crime prevention, but, as a participant from another focus group pointed out, there were insufficient resources to realise this potential:

> From an Intel perspective … We can identify problems, we can predict where we believe things are going to happen … and we can continue to say if we do this, then we should reduce crime. And we'll do it for 6 weeks, then stop because that's where the resources finish. And we've done that time and time again. So we've created this technology, or technology has helped us look at what's happened in the past and predict what's going to happen in the future crime-wise, but we don't have the resources to go to the next step … We've got police

collecting the information but not the time to actually go and act on what's been collected. (FG5: Intel/Tacticians)

Summary

The majority of police officers in the survey thought that information technology had made a great difference to police work. This response was particularly strong among respondents in higher ranks and those who had had a long period of service in the QPS.

For the majority of respondents, especially those in junior ranks, the use of crime reporting and transport registration systems was an integral part of their daily work. Respondents reported spending on average about 3 hours and 37 minutes per 8-hour shift using information technology to undertake various administrative tasks.

There was a perception among a proportion of the respondents (26–41%) that as a result of the introduction of information technology, they spent more time satisfying accountability requirements, doing paperwork, planning, organising or analysing information and supervising or checking the work of their staff. A similar proportion (25–39%) thought that information technology had led to police spending less time patrolling the streets, interacting with members of the community and informing citizens on the progress of their case. The majority of respondents, however, did not think that information technology had made any difference to the way they spent their time.

Respondents were generally positive in their assessment of the impact of information technology on their work. The majority thought that information technology had allowed them to work more effectively, made their work easier, and helped them cope with the amount of information police needed to do their work properly. Three out of four respondents agreed that information technology had led to an improvement in the quality of information, although only half thought that the security of information had improved. The majority thought that information technology had increased computer literacy as well as information sharing among police, improved communication between police officers and enhanced the professional status of police.

Four out of 10 respondents, however, thought that information technology had required police to follow unnecessary steps to get things done. This feeling was particularly strong among detectives, compared with officers in general or other duties. Respondents were ambivalent about whether information technology had limited the amount of discretion they have — although around 1 in 4 agreed, nearly 1 in 5 disagreed, and the rest were neutral. Focus-group discussions suggested that technology has made it a lot harder to take shortcuts or write files off. Survey

respondents were also ambivalent about whether information technology had taken some of the stress from their work — older and more senior officers were more likely to disagree. Part of this may be related to the feeling of information overload: nearly half of the respondents thought that information technology had led to information overload among police — older and more senior officers were more likely to feel this way.

Information technology did not appear to have changed the dominant style of policing in Queensland. Fewer than 4 in 10 respondents thought that information technology had led to a more problem-oriented police service or better proactive policing. Focus-group discussions suggested that the potential for smarter policing strategies was frustrated by the lack of time and resources and the inappropriate use of intelligence officers. Information technology had, however, facilitated successful proactive policing in the case of Maverick and MINDA for checking vehicles and people for outstanding warrants, leading to the collection of large amounts of unpaid fines.

The majority of survey respondents agreed that information technology had led to improved police service to the public. Focus-group discussions revealed that police procedures are now more transparent and responsive to the public as a result of the crime reporting system, since information about a case can be more easily accessed. Although nearly 6 in 10 survey respondents thought that information technology had led to improved police response to crime, some officers in the focus groups were concerned that police had become too reliant on technology for information. These officers lamented the loss of local knowledge and the retreat from hands-on methods for gathering intelligence.

Chapter 6:
Practical and technical problems

Problems encountered

Practical and technical problems inevitably arise in the implementation of any information technology system. How these problems are managed and resolved can affect the course and outcome of technological change. This chapter analyses some of the problems users reported to the researchers in the survey and in the focus-group discussions. It is not within the scope of this research to diagnose sources of problems; rather, our focus is on users' perceptions and their reported experiences of problems with information technology.

Survey respondents were asked to report on how often they had experienced problems with information technology, and, if they had experienced these problems 'occasionally' or 'frequently', to describe the most serious problem encountered and the impact of this problem on their work. Of the 482 respondents who answered this question, only 5% claimed to have 'never' experienced a problem. Thirty-four per cent reported that they 'frequently' experienced problems and 61 per cent reported 'occasional' problems. Respondents were also provided with an opportunity to make further comments at the end of the survey. Of the 114 respondents who offered additional comments, 79 (69%) made references to technical problems.

Table 6.1 summarises the problems identified, either as the 'most serious problem' or as a problem that the respondent felt the need to highlight in their 'additional comments'. Where a respondent cited the same problem in both questions, the problem was counted only once. In all, a total of 409 (81%) respondents identified at least one problem.

The most frequently reported problems were those associated with the overall performance of the hardware or systems; these were identified by 353 (86%) of the

Table 6.1
Problems experienced with the systems[a] (*n* = 409)

	Problem	Frequency	Per cent
Overall performance of the systems/hardware	Crashes/freezes computer or system down/outages etc.	287	70
	Slow system/computer	59	14
	General access problems	27	7
	Planned downtime	18	4
	Relates problems to Mac platform	10	2
	General software/system problems	4	<2
	General equipment problems	3	<2
TOTAL respondents referring to one or more of the above problems		353	86
Lack of integration of the systems		45	11
Adequacy of the resources	Old/outdated computers	14	3
	Insufficient number of computers	14	3
	Memory/power problems	11	3
	Printing problems	4	<2
TOTAL respondents referring to one or more of the above problems		33	8
Data quality	Data accuracy	19	5
	Data timeliness	6	<2
	System would not accept data entered	3	<2
	Poor data quality as a consequence of other technical difficulties	3	<2
TOTAL respondents referring to one or more of the above problems		30	7
Additional practical impediments to access and retrieval	Generally not user-friendly	10	2
	Key functions/spelling conventions	7	<2
	Lost information — reason not clear	6	<2
	Passwords	3	<2
	Searching/sorting problems	2	<2
	Virus	2	<2
TOTAL respondents referring to one or more of the above problems		29	7
Training and support services	Training problems	15	4
	Support problems	4	<2
Total		19	5
Communication system backlog (CRISP access)		7	<2

Note
a Multiple responses were given.

409 respondents who referred to a problem. All other problems were negligible in comparison: lack of integration of the systems (11%); adequacy of the resources (8%); data quality (7%); 'additional practical impediments to access and retrieval' (7%); problems with training and support services (5%); and communication system backlogs (2%).

Survey respondents were also asked to describe the impact of 'the most serious problem' on their work. Table 6.2 shows the impact on the respondents' work for all 'most serious' problems cited.

The impact on time and workloads was a recurring theme, with some variations within these two main themes. In terms of time-related impacts, 43 per cent of respondents referred to delays, wasted or lost time, or the speed at which a task can be completed. A small proportion (1.8%) referred to having to complete work in their 'own' (unpaid) time. From a workload perspective, 32 per cent implied that they were immobilised by the problem (e.g. 'unable to do work, had to wait', 'can't do anything'). Some responses (5%) referred to the need to redo work (e.g. 'had to start again — waste of time'; 'hours of retyping'), or to complete the work later in this or the next shift (1.5%). Also cited were impacts on the processing of offenders and offences (7% — e.g. 'unable to check if a suspect was currently wanted', 'delay in processing offender'), impacts on the emotions, with references to 'frustration' or 'stress' (7%), and lost information (6%). Only a negligible proportion of respondents (2%) reported finding ways around the problem (e.g. 'just do something else while it's fixed') or reported that the problem had little or no impact (1.8%).

System performance and computer resources

It is clear that the main problems reported by survey respondents related to the information systems' performance (table 6.1). Seven out of 10 respondents referred to computer or system crashes or freezes, system downtime, outages, shutdowns or breakdowns. According to focus-group participants, the main impact of downtimes

Table 6.2
Impact of 'most serious problem' experienced (*n* = 397)[a]

Impact	Frequency	Per cent
Time wasted	170	43
Work held up	128	32
Processing of offenders/offences	27	7
Emotions — frustration, stress etc.	26	7
Loss of information	23	6
Additional workload (redoing work)	19	5
Efficiency/effectiveness (non-specific)	19	5
Safety	10	3
Found ways around the problem	8	2
Little or no impact	7	<2
Impact on 'own time'	7	<2
Did work later or next shift	6	<2

Note
a Multiple responses were given. Only the more frequently cited impacts are reported.

or outages, whether planned or unplanned, was that police cannot do anything until the computers are back on line (FG1: GDs; FG2: OICs). Downtime was, therefore, considered to have accountability and crime-management implications and was said to be particularly frustrating when police 'have someone' (arrested an offender), but have to let the person go due to legislative limits on detention time (FG7: OICs; FG2: OICs; FG1: GDs).

The next most commonly reported performance problem was 'slow computers', although this was nominated by only 14 per cent of the respondents. Inadequacy of computer resources was also mentioned as a problem by a small proportion (8%) of respondents, who complained of an insufficient number of computers being available, and police having to use old or outdated computers with insufficient power and capacity. Focus-group discussions suggested that system performance and resource problems were seen to be interrelated:

> [the Bulletin Board] is a great system and all the information's there, but if you haven't got a computer … some of our computers downstairs can't access it so where's the benefit? … Even with an LC3, I mean you can have QPS but you mightn't be able to have Bulletin as well, and if you can get the Bulletin you might as well go and have cup of tea, lunch, go and visit someone, come back, by the time you get back it should have started … but if you want anything in a hurry … sometimes I'm lucky if … if I'm working on an LC3 in Microsoft Word I can't have Excel and anything else up and running because it's just going to … run down so dramatically that it's going to take forever to do a document. (FG5: Intel/Tacticians)

A computer that is old or has insufficient power was said to cause problems because: (a) some systems cannot run at all (FG5: Intel/Tacticians; FG6: GDs; Observation Report 1); (b) only one system can be run at a time (FG5: Intel/Tacticians), or (c) a system will run slowly (FG1: GDs; FG5: Intel/Tacticians).

Although only a small proportion of respondents nominated the inadequacy of computer resources as a problem, it did emerge as a significant issue in another part of the survey. When respondents were asked to give an assessment of their current computer resources, 74 per cent agreed that 'we don't have enough computers in our work area' (see table 6.3, next page). The problems appeared to be much more prevalent among respondents in the lower ranks and in general duties. For example, while less than half of the respondents in the rank of Senior Sergeant or Inspector agreed that they didn't have enough computers in their work area, the vast majority of FYCs (91%) and Constables (80%) agreed with the statement (table 6.3). General duties officers were more likely (80%) to agree that there were not enough computers, compared with detectives (66%) and respondents in 'other' duties (56%). These differences were statistically significant (chi-square test, $p < 0.05$). The frustration of

Table 6.3
Assessment of current computer resources (per cent of survey respondents)

	Per cent of respondents by rank						
	First Year Constable	Constable	Senior Constable	Sergeant	Senior Sergeant	Inspector	All
WE DON'T HAVE ENOUGH COMPUTERS IN OUR WORK AREA[a]							
Strongly agree/Agree (%)	91	80	68	59	33	25	74
Neutral (%)	3	10	12	13	22	13	10
Disagree/Strongly disagree (%)	6	10	20	29	44	63	17
Total respondents (*n*)	132	127	81	63	36	16	485
THE COMPUTERS IN MY WORK AREA ARE NOT POWERFUL ENOUGH TO RUN THE SYSTEMS THAT I NEED TO USE[a]							
Strongly agree/Agree (%)	56	65	65	60	36	6	58
Neutral (%)	33	25	20	22	25	38	26
Disagree/Strongly disagree (%)	11	10	15	18	39	56	16
Total respondents (*n*)	133	128	80	63	36	16	487

Note
a Chi-square test, $p < 0.05$.

working with an insufficient number of computers was often expressed by focus-group participants:

> I get cranky when I go to my desk and someone's at that computer, and I need to do something and they're doing something urgently … I've then got to find a computer somewhere else, it throws me out of kilter. (FG5: Intel/Tactician)

The power and capacity of computers was another dimension of the resource problem. While 58 percent of the survey respondents agreed that 'the computers in my work area are not powerful enough to run the systems that I need to use', this problem was again more prevalent among the lower ranks: only 6 per cent of Inspectors and 36 per cent of Senior Sergeants agreed that their computers were not powerful enough, compared with the much higher proportions (from 56 to 65%) of respondents in lower ranks who agreed with this statement (table 6.3). Respondents' opinions did not differ significantly according to duty on this issue.

These results are consistent with the IMD Client Survey and Service Quality Report, June 1998 (QPS 1998b), where 45 per cent of respondents indicated dissatisfaction with their access to computers. The results of our survey suggested that the problem may have become more salient in 1999, although the two surveys are not directly comparable. IMD data for the years 1996–97 to 1997–98 showed that the staff-to-

computer ratio in the QPS ranged from 0.4 : 1 in the Finance Division to 2.9 : 1 in one of the regions (see table 6.4). These data support the general perception of focus-group participants that 'civilians' and people working at headquarters had better computer resources than operational police (FG1: GDs; FG5: Intel/Tacticians; FG9: Specialist Investigators). For further discussion, see page 99 'Cultural conflict'.

In addition to problems with the power and capacity of individual computers, users perceived that the network was not always able to cope with the amount of traffic, resulting in slow or no access. 'Peak' system usage periods can exacerbate network performance inadequacies. Participants in one focus group said that Monday morning was particularly problematic for network access to do CRISP macro work[15] (FG7: OICs). Similarly, the RIMOs reported that much of the IT-based work was finalised in the last half hour of a shift, adding to the demand for both computer and network access: 'it is becoming very hard to address those peak periods, those change of shifts' (FG8: RIMOs).

The need to integrate the numerous stand-alone systems was discussed in chapter 3. Although only 1 in 10 respondents cited lack of integration of the systems as a 'problem' (11%, see table 6.1, page 69), the issue was raised repeatedly and in every focus group.[16] Perhaps the following best illustrates the problem:

Table 6.4
Ratio of staff to computers by region (1996–97 to 1997–98)

	Ratio of staff to computers	
Region	**1996–97**	**1997–98**
Far Northern	2.7:1	2.6:1
Northern	2.4:1	2.2:1
Central	2.2:1	2.0:1
North Coast	2.9:1	2.9:1
South Coast	2.1:1	2.0:1
South Eastern	2.8:1	2.5:1
Metro North	2.8:1	2.5:1
Metro South	2.7:1	2.5:1
State Crime Operations Command	1.6:1	1.5:1
Operations Support Command	1.7:1	1.5:1
Finance Division	0.4:1	0.5:1
Human Resources Division	0.8:1	0.9:1
Information Management Division	0.5:1	0.5:1
Administration Division	1.1:1	1.2:1

Source: IMD Client Survey (QPS 1998b, p. 53)

15 A keyword search of the CRISP data — mostly done by Crime Managers.

16 The issue was national integration rather than Service-wide integration in the Chief Superintendents' group.

> It's like a filing cabinet, you can't access one drawer to the other. You've got to open that drawer, get something, shut the drawer and go to the next drawer. That's how our index system works (FG4: Detectives).

For operational police, the 'drawers' were opened and closed so many times — the same information was entered repeatedly — that by the time the task was finished, 'you know him better than your mother [or] your father … ' (FG6: GDs).

Lack of integration was also reported as an issue for management and supervision because compliance checks were conducted in much the same way. One example from a focus group related to the checking of 'drugs matters': to check one item required accessing four or five systems. Thus, for 300 to 400 items in a period, the number of entries to be checked could be five times that number, which had consequences for time management (FG10: District Officers). There was general agreement among one group of OICs that the way to cope with the proliferation of databases that needed to be checked for compliance was to check random samples, otherwise 'you'd drive yourself mad'. However, it was acknowledged that this approach was less than satisfactory. For example, if one tape in a hundred was checked, 'there might be 80–90 problems' not being picked up (FG7: OICs).

Communication system backlog

Another problem that was more prominent in focus-group discussions than in the survey was the CRISP system backlog: less than 2 per cent of survey respondents identified this as a 'problem' (see table 6.1, page 69).

As noted in chapter 4, the CRISP database records all crimes that are reported to the QPS. Police officers call in the crime details to CRISP by telephone, either from the crime scene or as soon as practicable when they return to the police station. A civilian CRISP operator allocates a CRISP number to the report and records the details of the crime, as reported by the attending police officer, onto the CRISP database. There is also a CRISP supplementary form that can be e-mailed or faxed to CRISP when additional details arrive or changes have to be made.

Focus-group participants stressed that timely access to CRISP was extremely important for their work since the CRISP number was the link to 'everything'. For example, if they cannot get through to CRISP, they cannot complete any of the required indexes (FG4: Detectives). Furthermore, there is a departmental requirement that CRISP entries be submitted within 48 hours of the officers' attendance at the incident (FG4: Detectives). It was also suggested that the delays raised accountability issues. In one group we were told that a review was currently in place and officers had to justify delays over four hours: 'we have to put it on our logs now [to show] that we tried but we couldn't get through' (FG6: GDs).

> We did a study at XXX station and we averaged 12 ring-outs per officer during peak periods [to call CRISP] … the maximum was 36 times … so work out 12 by 2.5 minutes for a full ring-out session, that's how long an officer is sitting there doing nothing … and yet it's the officer who is held responsible for justifying the delay … (FG6: GDs)

Essentially, the problem was the time it took to get through by telephone to the operators. Some officers said that they dealt with the problem by putting the phone on speaker and continually redialling until an operator answered (FG6: GDs).

It is worth noting a comment by one senior police officer at this point: '[the] difficulty in getting through to CRISP is not insufficient resources, it's the management of them … we still haven't succeeded in getting officers to phone in reports through the course of their shifts, they all wait … when they get in, so you get a peak that you could never roster staff for … ' (Interview #4).

Our field observation did not find that CRISP access took as long as was suggested in the focus groups and in informal interviews in the field. The CRISP interactions observed took about half an hour to complete and, according to our observer, 'it didn't appear to be too difficult to make contact'. However, officers reported that the observed time was shorter than usual. Our observer noted that 'more officer time seemed to be spent filling out indexes, entering ARIs and completing supervisory paperwork than CRISP documentation'. It was acknowledged, however, that very few CRISP reports were generated during those periods of observation (Observation Report 1).

Our field observation also identified a number of other mechanisms for coping with the delays. For example, lists of stolen property generated at the scene of the crime could be faxed to CRISP, although the crime itself needed to be reported immediately to generate a CRISP number. Some officers put off their calls to CRISP until they had accumulated several crime reports and there was a lull in attending to calls for service, although this was rare and seemed to depend on the officer involved (Observation Report 1). An Officer in Charge at one station never filled out a CRISP form; instead, he rang and communicated details to the operators based on entries in his notebook, then printed out the CRISP report generated by the operator, and simply signed it as the official record.

The original intention was for the officer to be able to contact CRISP from the complainant's home; however, this was not always achieved because of the communication problem. Some focus-group participants said they felt embarrassed by this problem because the public might interpret the delay as a lack of professionalism on the part of the police (FG1: GDs; FG3: OICs). In addition, our field observation identified a concern with hygiene, which our observer considered quite justified. Telephones in a number of complainants' homes were 'filthy'; officers

therefore preferred to return to the police station to make the call to CRISP (Observation Report 1).

Future releases of Polaris will include a facility for Polaris to allocate a CRISP number online — without the phone call — so these delays should be eliminated. However, other performance assessments suggested that these complaints appear to be justified: according to the IMD Client Survey and Service Quality Report, June 1998 (QPS 1998b), only about half of the calls to CRISP are answered (see table 6.5).

One focus group also reported similar problems waiting for communications (channel 3) to do a check, which could take up to 20 minutes. During the course of this wait, the person being queried 'could be going off his brain, [asking] "when am I getting out of here?"'. This can be followed by a complaint for unlawful detention. This happens, not so much 'because technology's holding us up … [but] the lack of support on the technology'. According to this speaker, there was only one operator on channel 3 (FG1: GDs).

Data quality

As seen in table 6.1 (page 69), few survey respondents (7%) referred to data quality as being a problem. This is consistent with results from other parts of the survey, where a substantial majority of respondents agreed that information technology has led to an improvement in the quality (76%, see table 5.8, page 58), accuracy and timeliness (90% and 84%, see table 6.6) of information. Focus-group participants also tended to agree that IT had improved the quality of the information, although there were some data quality issues that were the subject of discussion.

Some tension was evident in relation to the CRISP data-entry process. Four focus groups expressed their frustration with the control of offence definitions by CRISP operators. A number of examples were given to illustrate this problem:

> A guy cut through a tin shed to break into premises, there was a motor bike in the way on the other side, he pushed the motor bike out of the way to do a B&E, and they [CRISP operators] categorised it as 'unlawful use of motor bike', because he pushed it two feet. (FG4: Detectives)

Table 6.5
Number of calls to CRISP received and answered (1995–96 to 1997–98)

	1995–96	1996–97	1997–98
Average number of calls received per month	77 141	72 403	76 693
Average number of calls answered per month	31 209	34 989	36 997
Average drop-out rate (per cent)	56	51	51

Source: IMD Client Surveys (QPS 1997, p. 28; QPS 1998b, p. 42).

Table 6.6
Perceived accuracy and timeliness of information

	Frequency	Per cent
IMPACT OF IT SYSTEMS ON THE ACCURACY OF INFORMATION (n = 476)		
A lot more accurate/somewhat more accurate	426	90
No difference	47	10
Somewhat less accurate/a lot less accurate	3	<1
IMPACT OF IT SYSTEMS ON THE TIMELINESS OF INFORMATION (n = 478)		
A lot more timely/somewhat more timely	403	84
No difference	61	13
Somewhat less timely/a lot less timely	14	3

The speaker said that he lost out in this case and the CRISP operator's definition prevailed. Officers were concerned that this kind of misclassification could have an impact on crime statistics (FG2: OICs; FG4: Detectives). Further CRISP offence codes are based on ABS classifications, not Queensland Statutes, which was perceived by some as a conflict between recording for crime management purposes and recording for the data needs of an external organisation (FG4: Detectives).

This frustration with CRISP's control of offence definitions was also evident in our observation. Our observer noted that:

> Some officers argue with the operators until some agreement is made, while others appear to have a lackadaisical attitude. They feel that they can't beat the system and why bother to try. They know the codes are inadequate and often wrong, but can't be bothered arguing the toss. (Observation Report 1)

Misinterpretation of the information by the CRISP operator, rather than outright disagreement with an officer, may also result in incorrect information being entered. Focus-group participants saw this as an accountability issue (FG3: OICs; FG1: GDs; FG4: Detectives). Additionally, it was noted in one focus group that, as new information comes to hand and is added to the system, the information can be entered in such a way that it is an inaccurate representation of the facts, as illustrated by the following example:

> If someone is put down as a 'suspect by description', when you then actually arrest the person and re-enter them, they put in a second offender. So they've got a 'suspect by description' offender then they've … got the guy you arrested as opposed to marrying it up or saying 'this is the same person'. So you've now got two offenders on the crime report when there's really only one. And it can get very confusing. And you get to court and they'll say 'well, where's the second offender?'. (FG4: Detectives)

Evidentiary problems can occur in court when the information on CRISP conflicts with what the officer says (FG3: OICs; FG4: Detectives).

Our observation also identified problems with the available CRISP codes, which were not always adequate for describing the situation. For example, a code of 610 [Community Assist] was applied to a boarding house disturbance because the officers provided information to the victim regarding his rights and the actions that he could take against the perpetrator of the offence. The police did not interview the perpetrator. The code did not reflect the numerous threats against the man's life (which was why the police were called), the actual fight that had taken place and that the blood of the perpetrator was found on the walls of his victim's flat. But, according to our observer, 'it was the best the police could do to describe the actions that they had undertaken' (Observation Report 1).

Whilst CRISP-related problems may have justified some officers' argument that police should enter their own data, focus-group participants noted that this, too, could lead to data integrity issues. Currently, officers entered data onto indexes themselves, but problems such as inconsistency of spelling can affect the integrity of search results (FG9: Specialist Investigators). Information contained on different databases can be contradictory when different people do the entries (FG10: District Officers). Lack of standardisation, particularly in the usage of CAD (FG1: GDs; FG7: OICs),[17] was also cited as an issue. According to participants in two groups, when offences were attended to 'on the fly', or as a result of a direct call to a station (that is, they were not tasked through CAD), some officers or stations would enter these jobs on the CAD system, others would not, thus affecting station statistics:

> … some people are putting on everything they do and some people aren't, but we use that as a tool to manage all sorts of things because it's the best thing we have (FG7: OICs).

Participants in one group also referred to inaccurate information being relayed to the officer on the road by communications (FG1: GDs). Officers expressed concern that this could put their safety at risk. In one instance observed by one of the researchers, officers attending a 'disturbance' in a boarding house were not provided with information of a similar disturbance between the same people at the same address just one week beforehand. Even the victim and the boarding-house manager assumed that the officers would be aware of this (Observation Report 1).

Timeliness of the information was also an issue in some focus-group discussions, particularly among officers at management level. Data entry backlogs of two, six and nine months were reported, and these were attributed to an inadequate level of resources being devoted to data entry (FG3: OICs; FG2: OICs; FG11: Chief Superintendents). A participant in one group also reported that there could be a time lapse of three to five days before a faxed modification was entered on the system

17 Since the data collection phase for this research a number of improvements to CAD have been made in this regard.

(FG2: OICs). Apart from affecting the accuracy of searches (FG1: GDs), these delays in data entry were also seen to influence whether a person got their 'just punishment' (FG3: OICs) and clear-up rates (FG2: OICs).

Ultimately, the information is 'as accurate as what's put into it' (FG10: District Officers). Despite the amount of checking that occurs, it was argued that the human factor was sometimes overlooked (FG5: Intel/Tacticians) — there can be a perception that information technology is the information, and that sometimes 'if it wasn't accurate you wouldn't know it wasn't accurate … ' (FG10: District Officers):

> Once it's on that computer, somehow they seem to forget that it was a human being that entered the information, and so the computer is always right. So, if the original data is inaccurate, that can become a huge problem [interruption: especially in court] (FG4: Detectives)

The issue of data quality was also raised by information technology managers and the CJC. For example, an information technology manager suggested that the amount of useable data was in the vicinity of only 25 per cent (Senior Information Technology Manager, Interview #10). An officer described the data quality checks that were in place:

> … everything should go back through the OC … the warrants are sent back through the OC to the person that does the actual work … if you do a QP9 (court brief) even when it's electronic you will send that to a brief checker and he will go through that court brief and if that's no good he will send that back to him electronically. He'll get it fixed and it will come back to him, and then it goes electronically to the Prosecutions Section who will go through the QP9 and if it's not right and they want something else they'll send it back to the brief checker back to the [unclear] to have it fixed up, so that (you know) there's a quality check, there's two quality checks along the way for a court brief, so we are, we are a little bit paranoid about computer systems having quality information in it. (Senior Information Technology Manager, Interview #5)

Despite these apparently rigorous checks, the speaker acknowledged that 'it's absolutely impossible for people to get it 100 per cent right … human error will always play a part and it's part and parcel of life. But we certainly try our best … ' (Interview #5).

Problems with data quality were highlighted in the Beenleigh Calls for Service Project (CJC 1998a). One objective of this project was to improve the local Incident Management System (IMS) so that it could be used as a problem-solving tool. Despite ongoing enhancements, the evaluation identified that throughout the history of the project accuracy remained low (especially in the incident address field). A report emanating from the project (*The Cost of First Response Policing*, CJC 1997b) pointed to poor address definition, inaccurate time recording and inappropriate or

inaccurate classification of calls as persistent problems, and suggested improvements in the form of:

- better design of information systems (such as employing look-up tables)
- formulating and documenting consistent recording and classification procedures
- training communications room staff and police officers on the application of these procedures
- instituting quality-control processes and periodic auditing to ensure compliance with these procedures (CJC 1997b, p. 9).

Other design problems

A small proportion of survey respondents (7%) referred to general problems with the user-friendliness or format of the systems, problems of lost information, problems with searching or sorting, problems with inconsistent key functions or spelling conventions between systems, the proliferation of passwords, and the problem of viruses (see table 6.1, page 69). These problems were raised in eight of the focus groups.

Participants complained of inconsistent spelling conventions and incompatible keystroke commands, which were partly due to the lack of system integration. For example, in some systems, entering an approximation of a name (e.g. 'Kerry' for 'Kerrie') would achieve the desired result, but, in other systems, such as the Domestic Violence index, an exact spelling was required (FG2: OICs). Centralised data entry (CRISP) was considered an important mechanism for ensuring consistency of keywords to enable searches to be undertaken at a later date (FG4: Detectives). An example of incompatible key functions was the use of PF6 to go back in the Correspondence Index, but, in the Tapes Index, it was PF4 (FG7: OICs).

The problem of multiple passwords was mentioned in four focus groups. Some officers in the field told our observer that it was simpler just to use someone else's ID to conduct their searches if the program was already open (Observation Report 1).

Officers also expressed frustration with the time spent scrolling the Bulletin Board (FG2: OICs; FG5: Intel/Tacticians) and CRISP (FG6: GDs) to find information, and the lack of access to electronic CAD data (FG6: GDs; FG7: OICs). Some participants complained that the QP9 (court brief) now took longer to complete than it did with a typewriter because of the need to wait for each screen to come up (FG1: GDs; also FG6: GDs). A recent change to the traffic accident system was considered a retrograde step, since a change in the search capabilities made it impossible to search for incomplete accident reports. The group was in general agreement that this was 'a bad move' that went ahead with 'no consultation' (FG7: OICs).

Training and support services

Only 5 per cent of survey respondents mentioned information technology training and support services as a problem (table 6.1, page 69). Survey respondents were generally satisfied with the adequacy of the training. Of the 419 who reported that they had received training, 69 per cent said the training was adequate for their needs. This perception differed significantly by rank, with respondents in the lower ranks more likely to report satisfaction (chi-square test, $p < 0.05$). More than three-quarters of FYCs (83%) and Constables (76%), and almost two-thirds of the Senior Sergeants (61%) reported that the training was adequate, while only 54 per cent of Senior Constables, 55 per cent of Sergeants and 40 per cent of Inspectors felt the same way. Respondents were more equivocal about their satisfaction with support services: 55 per cent (266 of 487) said they were satisfied with the support services, a large proportion (42%) were neutral and a small proportion (4%) dissatisfied. This perception also differed significantly by rank, but in the opposite direction, with senior ranks more likely to report satisfaction (chi-square test, $p < 0.05$): FYCs/ Constables (50% satisfied), Senior Constables/Sergeants (62%), Senior Sergeants/ Inspectors (67%).

Part of these variations by rank may have been due to differential access to training and support services, or differences in learning styles. When survey respondents were asked to identify how they learnt to use the information systems, the most frequently reported methods of learning were 'trial and error' (74%), formal training at the Academy (64%), informal help from colleagues (55%), TAFE courses (40%), and computer-based training packages (31%; see table 6.7, next page). Most learnt by more than one method, with only 13 per cent of the respondents reporting that they learnt by one method only. A small proportion of respondents (around 1 in 10) did not appear to have received any formal training in information technology. [18]

Variations in learning methods emerged when the top four methods used were broken down by rank (see table 6.8, next page). 'Trial and error' was the most frequently reported method of learning for all ranks, except Constables and FYCs, whose most frequently reported method of learning was 'formal training at the Academy' (Constables 85%, FYCs 98%). 'Informal help from colleagues' was the second most frequently reported method for Inspectors (81%), Senior Sergeants (83%), Sergeants (64%) and Senior Constables (42%). Computer-based training (CBT) was reported by less than half of respondents of all ranks. Of the top four methods of learning, CBT was the only method that did not show significant differences by rank.

18 This figure was estimated in two ways. In response to the question, 'If you received formal training, was the training adequate for your needs?', 14 per cent of respondents (67 of 486) claimed not to have received any formal training. Alternatively, 13 per cent of respondents (63 of 493) reported learning only by 'trial and error' or 'informal help from

Table 6.7
Methods of learning to use the systems (*n* = 493)[a]

	Frequency	Per cent
Trial and error	366	74
Formal training at the Academy	316	64
Informal help from colleagues	270	55
Other — TAFE	195	40
Computer-based training package (CBT)	151	31
Formal training provided by the Region	91	19
Assistance from the Help Desk	67	14
Formal training provided by the station	49	10
Formal training provided by HQ	20	4
Other — databases such as Hep B index, Bulletin Board, manuals, training	12	<2
by staff	3	<2
Assistance from the Expert Support Unit (ESU)		

Note
a Multiple responses were given.

Table 6.8
Top four methods of learning by rank[a]

Most frequently cited method of learning	*Rank of Respondent (per cent)*					
	First Year Constable	Constable	Senior Constable	Sergeant	Senior Sergeant	Inspector
1	Academy[b] (98%)	Academy[b] (85%)	Trial and error[b] (84%)	Trial and error[b] (87%)	Trial and error[b] (92%)	Trial and error[b] (100%)
2	Other — TAFE[b] (72%)	Trial and error[b] (72%)	Informal help from colleagues[b] (42%)	Informal help from colleagues[b] (64%)	Informal help from colleagues[b] (83%)	Informal help from colleagues[b] (81%)
3	Trial and error[b] (59%)	Informal help from colleagues[b] (51%)	CBT (41%)	CBT (38%)	CBT (33%)	Formal training provided by region[b] (44%)
4	Informal help from colleagues[b] (53%)	Other — TAFE[2] (47%)	Academy[b] (40%)	Formal training provided by region[b] (32%)	Formal training provided by region[b] (33%)	Help Desk[b] (19%)
Total respondents	134	130	80	63	36	16

Notes
a Multiple responses were given.
b Significant differences by rank (chi-square, $p < 0.05$).

These results suggest that the vast majority (over 80%) of senior police from Senior Constables to Inspectors learnt how to use information technology through 'trial and error', and a substantial proportion (42 to 83%) through informal help from colleagues, rather than through formal training. Moreover, a sizeable proportion of these senior officers (24% of Senior Constables, 27% of Sergeants, 25% of Senior Sergeants and 38% of Inspectors) reported learning by these informal methods alone. It is not clear from the survey whether senior officers did not have adequate access to formal training or they preferred not to make use of the available formal training.

Focus-group participants' accounts varied considerably both within and between groups about what training was available and how much training an individual received on a particular system. Despite the disparities in experience, most participants reported that major systems such as CRISP and Polaris came with training at implementation, but, for other systems, sometimes only CBT (FG6: GDs) or no training was offered (FG8: RIMOs; FG6: GDs). After the initial training (if any), officers usually 'learnt by doing' or from colleagues, although some officers mentioned the availability of training for Polaris upgrades (FG4: Detectives; FG9: Specialist Investigators). Some officers found it useful to consult manuals, ring the 1-800 support numbers or the Help Desk (FG3: OICs), while others preferred to pay visits to information technology support personnel (FG4: Detectives; FG5: Intel/Tacticians).

A number of factors may have been responsible for police not getting information technology training. First of all, the method of training was an issue raised by one focus group: officers had a preference for the small group, on-site training format for Polaris over the 'up front, didactic' format for CRISP (FG2: OICs). CBT was seen as positive by some group participants because it is self-paced and obviates the need to attend lectures (FG4: Detectives). It was seen as 'dynamic, enjoyable, and can be done in an officer's own time' (FG7: OICs), particularly useful for systems such as Police Powers and Polaris that required 100 per cent compliance (FG7: OICs). However, CBT was not always high on an officer's list of priorities (FG6: GDs), and its effectiveness may be dependent on motivation. As one officer pointed out, 'the CBT training, well, if you don't have to do it, why do it?' (FG5: Intel/Tacticians). One focus-group participant said that CBT was usually done the day before the training period ended, when there was a realisation that 'you haven't got enough hours up, and then you think, "Oh shit, I've got two hours of CBT to do" … so you sit down and you go … "Oh yeah that's my two hours done, tick, how many more do I need?" … and that's when you do your training … it's not done for the right reasons' (FG6: GDs). Another problem was that CBT could not be accessed by most computers (Observation Report 1) as they did not have sufficient power and capacity (FG5: Intel/Tacticians). Poor computer literacy could be a problem with CBT, and the cause of some embarrassment in training classes, thus impeding learning (FG4: Detectives).

There was general agreement that motivation was a contributing factor to how much training officers undertook, or how much officers chose to learn (FG8: RIMOs; FG10: District Officer; FG11: Chief Superintendents; FG9: Specialist Investigators):

> … if you didn't want to learn something, you don't learn. And that's become … the dinosaur feature. (FG9: Specialist Investigators)

Time constraints also affected the extent to which police attended information technology training. Some officers thought that there was not enough time to do training (FG10: District Officers; FG6: GDs; FG7: OICs; FG5: Intel/Tacticians), or that insufficient time was allocated to training sessions (FG1: GDs; FG7: OICs; FG2: OICs). Others thought there was 'more than enough training at times' (FG11: Chief Superintendents), contributing to 'training overload':

> I think one of the huge problems … in relation to all these systems and a lot of other things besides the information systems, is that all that is so time-consuming that we haven't really got time to be police anymore. We're far too busy training and making sure that we're complying with the compliance … (FG6: GDs)

Another issue raised during the focus-group discussions was that, at times, information technology training was combined with training in general. One participant bemoaned the teaching methods and limited time allocated to Police Powers training: it was 'the most important legislation change in Queensland's history and we get a day and a half' (FG5: Intel/Tacticians). The perceived imbalance of training priorities was raised as an issue in one group: too much time was spent on namby pamby training (the example given was of sexual harassment/equal employment opportunity (EEO) training) that took police off the road and was perceived to have little relevance to the job, whereas not enough time was spent on practical, job-related training, such as information technology training (FG1: GDs).

While it was compulsory for police to undergo procedural training in relation to new systems, only two days per month were allocated to each police officer for training overall (Interview #3). This included all aspects of policing (such as new legislation), not just information technology-related training. These and other demands (such as court appearances and operational requirements)[19] can make attendance at training difficult and it cannot be guaranteed that all officers will be adequately trained in all procedures or programs in a timely fashion. An information technology manager suggested that 'the only thing they're guaranteed on training is firearms training. It takes priority — [yet] it's possibly the least-used piece of equipment' (Interview #12).

The timing of training was considered crucial: if training was provided too early before implementation, training or skills 'decay' could result (FG3: OICs; FG2: OICs;

19 ' … any training situation is going to be impacted [on] by the unknown — we're police — we can't predict when a disaster's going to happen or whether some maniac is going to do something …' (Interview #5).

FG9: Specialist Investigators; FG4: Detectives). 'Skills decay' could also occur with a lack of continuous usage, which was reported as an issue in the higher ranking groups (FG10: District Officers; FG11: Chief Superintendents). Linked with this was the complaint that there was insufficient training for skills maintenance and changing job functions (FG5: Intel/Tacticians; FG6: GDs).

One group of OICs was concerned about the lack of coordination of training. Examples cited included the Polaris upgrade, the new *Road Rules Act* and firearms, which all required training to be completed within a given period of time (FG2: OICs). This same group also expressed concern about information overload: the amount of information one can process and retain when training is 'full-on' for implementation. The impact of training on rostering was an issue for one group of managers:

> The rostered shift only goes so far, and we've got that many people off on training now that we can't run our operations and train at the same time, so really the opportunity cost of putting people through courses is becoming crucial. (FG10: District Officers)

Individuals could miss out on formal training for a variety of reasons. Even with 100 per cent training compliance requirements (for example, for Police Powers and Polaris), some could still miss out on training. A RIMO mentioned receiving an inquiry from an officer seeking assistance with Polaris — this officer had been promoted to an in-charge position:

> I gave them guidance on where to get manuals but it's horrifying that someone can get to that level … and must have never accessed the system before. He's missed the training obviously in all that time … (FG8: RIMOs)

One person said he had missed out on Polaris training because he had other commitments that took priority (FG5: Intel/Tacticians).

Legislation and accountability requirements often dictate that information systems be introduced statewide in a 'big bang' manner. Polaris, for example, was switched on simultaneously across the State, but a training coverage of only 80–85 per cent was achieved by that time (Information Technology Manager, Interview #5). An information system officer noted that:

> You can only access Polaris if you're trained and have been accredited by your trainer as having been trained … then you go through Security and you're given access … provided you keep modifying your passwords … you can maintain access … If you simply do not use Polaris for a long period of time, you'll lose access and you have to go back through the security process (but not the training process). (Interview #5)

CRISP, on the other hand, was rolled out district by district, region by region, over a period of three to six months. Training for that program was also problematic,

however, in that either it was offered too early and the information was lost before it could be used (Interview #5) or there was resistance from officers to attend the courses because, until CRISP, there had been no perceived benefits for police becoming involved in IT. As an information technology manager pointed out, CRISP was the first system that they 'had to use in order to do their work':

> we turned the corner with CRISP … coppers started using it … and said 'wish I'd gone to the training course because this is really good stuff'. (Interview #14)

Subsequent releases of Polaris, e-mail and the Bulletin Board have reinforced the importance of information technology training to police ('those sorts of things just blew the coppers away' — Interview #14).

Location was a factor that may have affected the availability of training and support services. It was reported in one focus group that those who were out west had less access to training and support services (FG4: Detectives). However, rural OICs were very positive about the support available for training, saying that for smaller stations there are 'a multitude of freecall numbers' to ring. The TRAILS support by way of a 1-800 number was considered particularly helpful. There was minor disagreement about the support available for the QPS system; however, the general tone was that the QPS Help Desk has been very good (FG3: OICs).

While the survey results showed no significant differences in satisfaction between respondents from metropolitan or suburban locations (54% were very satisfied/quite satisfied with the support services) and those from provincial cities or rural areas (57% were very satisfied/quite satisfied), two focus groups told us that support was much easier to access if the information technology people were physically closer (FG4: Detectives; FG5: Intel/Tacticians). Furthermore, RIMOs did not think it was their role to be on call, although they felt some obligation to respond to after-hours calls. This was a pressure more often felt by regional rather than metropolitan RIMOs, since, in the metropolitan area, ISB staff were on call (FG8: RIMOs).

Differences in satisfaction with support services may depend on whether the help sought was in relation to system usage (training-related) or technical problems, or on the type of technical problem, the expertise of the person at the Help Desk or the time of day help was sought. We saw previously that one group expressed satisfaction with training-related support, while another group was critical of the lack of technical support available out of hours when the system went down (FG1: GDs). One participant in the RIMOs group said that there were varying levels of expertise at the Help Desk. Another said that whether help was forthcoming depended on who you got on the phone (FG8: RIMOs).

General attitudes towards information technology

Despite the practical and technical problems that users experienced with the various information systems, there was never any suggestion among the survey respondents or focus-group participants that information technology should be abolished. Indeed, as we saw in chapter 5, users perceived a number of gains as a result of the introduction of information technology. From the focus-group discussions it would appear that information technology was appreciated as a tool for information management. In fact, officers thought that they would not be able to cope with all the information without such technology. What they wanted was more adequate resources, more user-friendly systems, faster access and more efficiently managed information.

A RIMO said that the problems for police were not so much the systems but:

> … the problem of not being able to get access to the systems … the computers themselves (FG8: RIMOs).

We mentioned earlier that some officers had particular problems with, for example, the search functions in some systems or some system-specific navigation difficulties, but, overall, the complaints were not so much about the individual systems, but problems of access. These problems were related to poor system performance, which was caused by inadequate resources, lack of integration of the systems and delays in accessing CRISP operators. In general, officers found the indexes useful, but complained about the cumbersome process of getting to the information (FG4: Detectives). When asked whether they would get rid of information technology, the answer from a participant in this group was: 'not the information, just streamline the information'.

This distinction between individual systems and the systems *in toto* may help to explain the large proportions of neutral responses to the survey questions regarding the ease of use of the systems and whether the respondent was 'happy with the way the systems work now'. Fewer than half the respondents agreed that they were 'happy with the way the systems work now' (45%, 217 of 488), and that the 'systems were very easy to use' (46%, 227 of 489), while a large proportion remained neutral on each of these statements (36% and 32% respectively).

Although there were no significant rank differences in satisfaction with the way 'the systems work now', rank differences were statistically significant in the perception of ease of use (chi-square test, $p < 0.05$). There was a tendency for the proportions to decrease with rank: the highest proportion of those who agreed that the systems were easy to use were Constables (58%), followed by FYCs (52%), Senior Constables (41%), Sergeants (41%), Senior Sergeants (31%) and Inspectors (25%).

Survey respondents were asked whether there were any aspects of the systems that they avoid using, and to give examples and their reasons for avoidance.

Only 16 per cent of respondents (77 of 476) reported that there were some aspects of the systems they avoided using. Of the 77 respondents who reported avoidance, the systems avoided were: NEPI (23); Polaris/warrants (13); training packages or online help such as Advance, CBT, Help (9); TRAILS/TIRS/Traffic accident system (9); and the Bulletin Board (4). Twenty-two of the 77 did not nominate a system.[20] Only 10 per cent of FYCs reported that there were aspects of the systems that they avoided using, but avoidance appears to increase with rank: Constables (11%), Senior Constables (14%), Sergeants (18%), Senior Sergeants (42%) and Inspectors (47%). These differences were statistically significant (chi-square, $p < 0.05$).

The main area of avoidance reported in the focus groups was in relation to e-mail messages, where 'deletion' was reported as a mechanism for coping with the profusion of messages (FG5: Intel/Tacticians; FG2: OICs). This practice raised the anxieties of participants in one group, the concern being that official e-mail may be being deleted (FG6: GDs). However, the e-mail system itself was not avoided.

Cutting corners with minor matters may be a form of avoidance. However, as discussed in chapter 5, the systems were designed to make it difficult, if not impossible, to circumvent the required steps (FG4: Detectives; FG5: Intel/Tacticians).

Among the 77 survey respondents who acknowledged avoiding parts of the systems, the most frequently cited reason for avoidance was related to the lack of skills (40%).[21] These included reasons such as inadequate knowledge, lack of training or inadequate training. The next most frequently reported reasons were connected with the ease of use: 'too difficult to use' (26%) or 'too time-consuming/slow' (21%). Fifteen respondents (19%) said that they avoided the systems because they had no access or no need to access them. Other reasons for avoidance included: no password/password expired (9%), the information is useless (5%), deskilling due to lack of use (3%) or too frustrating (1%). Four of the 77 did not provide a reason for avoidance. These results suggested that users may be less likely to avoid these systems if officers were more skilled in information technology (e.g. through better training), if the systems were more user-friendly and access were less time-consuming.

20 Multiple responses were provided; only the most frequently nominated systems were reported.

21 Multiple responses were reported.

Summary

The introduction of information technology has brought with it a number of practical and technical problems for police. The vast majority of survey respondents told the researchers that they had experienced problems with the information systems 'frequently' (34%) or 'occasionally' (61%). These problems also dominated much of the focus-group discussions.

The most frequently reported problems were associated with the performance of the systems. These ranged from planned or unplanned downtime and access difficulty to software and hardware problems. Focus-group discussions suggested that poor system performance was caused or exacerbated by: the inadequacy of computer equipment, both in availability and in power; the lack of integration of the systems; and severe communications backlog in relation to CRISP. There was also some concern with the accuracy of the data, especially the inconsistent use of CRISP codes, as well as various minor design flaws.

While respondents reported being generally satisfied with the training and support services associated with information technology, senior officers were less likely to find training adequate but more likely to report satisfaction with support services than junior officers. One significant finding was the high percentage of respondents, especially among the senior ranks, who reported that they learnt to use information technology through informal methods such as 'trial and error' and 'informal help from colleagues', rather than through formal training. It is not clear from the survey whether senior officers did not have adequate access to formal training or they preferred to not make use of the available formal training. We estimated that 1 in 10 officers did not receive any formal training in information technology. This could be due to a number of reasons, including the inability to use CBT because of inadequate equipment or poor computer literacy, lack of motivation, time constraints, inappropriate timing relevant to the release and/or use of the program, lack of coordination, or insufficient time to train staff before the statewide introduction of new technology.

Many of the technical problems that were raised by survey respondents and focus-group participants in this research echoed results of the annual surveys of operational police and managers conducted by the IMD. Findings reported in 1997 (QPS, 1997), for example, suggested that, while the majority (72%) felt that the performance of the computer systems had improved, more than half (58%) thought that the computer system had performed poorly or inadequately during the year. Poor performance was attributed to downtime, lack of system integration, lack of training and lack of computers. While in 1997 operational police's satisfaction with many IMD services had improved, the majority of respondents were only partially satisfied with the services. Furthermore, as few as 35 per cent felt that their level of

knowledge of general policing systems was good, while 20–25 per cent said that their knowledge of such systems was poor.

We have seen in this chapter that, in spite of all the problems encountered, police who participated in the study showed little resistance to the technology. Only a small proportion (16%) reported avoiding some aspects of the systems. In the main, police officers appeared to have accepted information technology as a useful tool for their work. Far from being Luddites in the Information Age, officers saw more powerful, faster and more accessible technology as the answer to their problems. This acceptance signals a potential transformation of the workplace and the organisation as a whole. The impact of information technology on the QPS as an organisation is the subject of the next chapter.

Chapter 7:
Impact of IT on the Police Service

This chapter examines the impact of information technology on the QPS as an organisation. It has already been pointed out in chapter 5 that the majority of survey respondents thought that information technology had made a great difference to police work. Police in our survey were generally positive in their reception of the technology, in spite of the many technical problems encountered in their use of this technology (see chapter 6), and in spite of their perception of having to spend more time on paperwork. Not only did police officers accept information technology as an integral part of policing, the majority thought that technology had made their work easier, helped them to work more effectively and led to improved police service to the public. In this chapter, our focus moves from operational policing to the structure and culture of the police organisation. We investigate the extent to which information technology has changed workplace relations, management and supervisory practices, organisational culture, and the QPS's relations with external agencies.

Workplace relations

Survey respondents rated positively the impact of information technology on workplace relations, communication and effectiveness. Table 7.1 (next page) shows that the majority agreed that information technology had led to improved information sharing between workers (70%) and improved communication between workers (58%); it has also increased their area's effectiveness (53%). Fewer than 10 per cent of respondents disagreed with those statements. Similarly, respondents tended to agree that information technology has allowed people to work more cooperatively (47% agreed v. 7% disagreed) and created a more positive work atmosphere (30% v. 13%), and disagreed that it has caused conflict between people (28% disagreed, 13% agreed). However, a fair proportion of the respondents neither agreed nor disagreed with these statements (see table 7.1, next page).

Table 7.1
Impact of information technology on workplace

Information technology has …	*n*	*Per cent of respondents* Strongly agree/ agree	Neutral	Disagree/ strongly disagree
… led to improved communication between workers.	473	58	35	8
… led to improved information sharing between workers.	474	70	25	5
… allowed people to work more cooperatively together.	473	47	46	7
… created a better work atmosphere.	474	30	57	13
… caused conflict between people.	473	13	59	28
… increased my area's effectiveness.	471	53	41	6

Improvement in communication between workers was largely the result of the availability of e-mail. One focus-group participant (FG5: Intel/Tacticians) gave an example of where e-mail has worked well for him and saved him a lot of time. He was involved in a coronial matter that required getting statements from across the State. Apart from the first contact phone call, he was able to obtain all the statements via e-mail. Others in the group agreed that e-mail is an excellent tool for people who do shiftwork (FG5: Intel/Tacticians). Participants admitted, however, that the disadvantage of e-mail is that workers tend to lose one-to-one contact with each other. E-mail can also create more work because it is easy to involve a great number of people in decision making. However, as another focus group pointed out, e-mail facilitates effective teamwork and information gathering:

> The team I work with at the moment are in three different parts of the building … most of our interaction is done by e-mail, and once a day we'll get together. So we're e-mailing each other documents, questions, answers. We don't even use the phone virtually any more, it's just straight e-mail. [Q: Overall, is that positive or negative?] As far as teamwork, it has a positive effect, and I think it still remains positive if you still have that personal interaction on a regular basis.
>
> We have a project where we've got pseudo-members of our team all round Australia and in America giving us advice on our project, and it allows us to feed them and get information back within 24 hours, without ever having face-to-face contact. (FG9: Specialist Investigators)

Table 7.2 summarises survey respondents' opinions of the impact of information technology on their relations with supervisors. The majority agreed that information technology has led to a closer scrutiny of their work by their supervisors (55%), and that information technology has made their supervisors more aware of their day-to-

day activities and workload (52%). A smaller proportion (35%) agreed that information technology has improved communication between them and their supervisors, but respondents were equivocal about the statement that information technology has led to a reduction of face-to-face contact with supervisors — 29 per cent agreed, 48 per cent were neutral and 23 per cent disagreed. More than a third disagreed that information technology has created conflict between them and their supervisors; only 7 per cent agreed.

These results do not show a great deal of variation by rank, except that respondents in the ranks of Sergeant and Senior Sergeant were significantly more likely to agree that information technology has improved communication between them and their supervisors: FYCs (35% agreed), Constables (25%), Senior Constables (36%), Sergeants (46%), Senior Sergeants (53%), Inspectors (31%). Sergeants (40%) and Senior Sergeants (42%) were also significantly more likely to agree that information technology has reduced face-to-face contact with supervisors: FYCs (25%), Constables (23%), Senior Constables (33%) and Inspectors (31%). There were also few variations by duty, except that general duties officers among the respondents were less likely to disagree that information technology has led to improved communication with their supervisors (8% disagreed or strongly disagreed, compared with 12% of detectives and 18% of 'other duties'). Detectives were more likely to agree that information technology has made their supervisors more aware of their day-to-day activities and workload (68%) compared with general duties officers (53%) and officers in 'other duties' (41%).

Table 7.2
Impact of information technology on relations with supervisors

		Per cent of respondents		
Information technology has …	***n***	**Strongly agree/ agree**	**Neutral**	**Disagree/ strongly disagree**
… led to closer scrutiny of my work by my supervisor.[c]	473	55	40	6
… made my supervisor more aware of my day-to-day activities and workload.[b]	473	52	37	11
… improved communication between me and my supervisor.[a,b]	473	35	54	11
… reduced face-to-face contact with my supervisor.[a]	473	29	48	23
… created conflict between me and my supervisor.	473	7	57	36

Notes
a Rank differences are statistically significant (chi-square, $p < 0.05$).
b Duty differences are statistically significant (chi-square, $p < 0.05$).
c Chi-square test for significant differences for rank could not be conducted since more than 20 per cent of cells had an expected frequency of <5.

Management and supervision

As described in chapter 5, a substantial majority of respondents in the survey thought that information technology had made a great difference to police work. Some of this difference is reflected in respondents' reported use of time: Senior Constables and above were more likely to report spending more time on accountability requirements, paperwork, planning, organising or analysing information, and supervising or checking work of staff (chapter 5). As an Officer in Charge in one of the focus groups explained:

> Eighty per cent of our time is probably consumed in doing all this sort of stuff … There's huge benefits in [information technology], but we haven't got time to use it … There's accountability issues … and in order to fulfil what we're supposed to under the OPM, you've got to spend half the day doing this sort of stuff … I could spend six or seven hours a day just doing compliance without even looking at police work. OICs of bigger stations probably would need half a dozen staff to do that properly. Nobody does it properly — we're all aware of that. It's very frustrating. I think the job in general needs to aim towards having experts in certain areas who we can access rather than us being an expert in everything. We have to be a 'jack of all trades' at the moment, and I don't think that's conducive to being good police. (FG6: GDs)

Because the information technology systems were not very user-friendly, it was pointed out that 'management' often found that they could not afford the time to make effective use of information technology systems and, as a result, the task of summarising the information fell on more junior staff: 'it's a quick reference for them, but time-consuming for the officers. Grossly inefficient' (FG4: Detectives).

There was a general feeling that additional reporting and accountability requirements came with the advent of information technology. Two-thirds of the survey respondents agreed that information technology had required them to report on their activities more frequently (68%) and made them more accountable for their actions (66%). When these results were broken down by rank, it appeared that the middle ranking respondents were more likely to agree that information technology required them to report on their activities more frequently: FYCs (64% agreed), Constables (67%), Senior Constables (75%), Sergeants (81%), Senior Sergeants (50%), Inspectors (67%). With the second statement, the trend was slightly different, with the higher ranks more likely to agree that information technology had made them more accountable for their actions: FYCs (68% agreed), Constables (67%), Senior Constables (63%), Sergeants (71%), Senior Sergeants (53%), Inspectors (80%). The Senior Sergeants among the respondents were least likely to agree with both statements.[22]

22 Note, however, that these results may not be generalisable to other samples. Chi-square tests of significance could not be conducted as, for both statements, more than 20 per cent of cells had an expected frequency of less than 5.

Several focus-group participants pointed out that it was, in fact, the need for accountability that caused the additional workload, not the information technology systems. One officer concluded that 'the amount of time spent on the computer isn't because of information technology, it's because of legislation that we've got to do' (FG9: Detectives). Others added that 'if we didn't have the information technology to meet those regulations, we'd be even slower', or 'we'd be stressed out that much that you'd have half the Police Service on stress leave'. To achieve the same level of reporting using the old manual system would have been impossible, as another officer said, 'like, even though QUID was bad, it replaced probably six people just doing manual collation cards, and they were only doing it for a very small amount of input— you try to collate an intelligence system with cards that QUID had, [it's],you know, astronomical' (FG9: Specialist Investigators).

There is no doubt that information technology has given police supervisors a greater capacity to scrutinise the work of their staff, but whether this capacity has been used effectively is debatable. One supervisor in a focus group described how he used information technology to check his staff's work. He said it was a 'tick and flick' process: he went through a number of systems to check for outstanding tasks — MNCR system for correspondence, QTAOS system for traffic accident reports, the exhibit register, the property register and so on. Then he would sit down with the officer and ask why each was not done, writing down the excuse in each case. He did this once every four weeks, but said that 'it's useful for the administration, but not for me personally' (FG1: GDs).

An OIC in another group explained that the new IMS allows supervisors to check where their cars are, what their officers are doing, how far they have got in their CRISP report and whether they have done their job properly:

> With IMS in relation to domestic violence, officers there might not be doing the right things as far as the legislation goes. There's a prosecution index to check the work rate of first years to see what sort of arrests there have been, and check on the court dates, and [you can] go and watch them in court and give them some feedback on their efforts. (FG2: OICs)

However, this officer said that he didn't really use the IMS, because he didn't have time to do it.

There was some concern within one focus group that, as a result of information technology, management would become more impersonal as managers come to rely on e-mails rather than personal interactions for communication (FG9: Specialist Investigators).

Accountability, management and decision making

Table 7.3 summarises survey respondents' views of the impact of information technology on accountability, management and decision making within the QPS.

Accountability

When respondents were asked in general terms whether information technology had led to improved police accountability, 6 out of 10 agreed, although a similar proportion also thought that information technology had led to an overemphasis on accountability (table 7.3). These results do not vary significantly by duty, but respondents at the rank of Inspector were much more likely to agree with both statements than the officers in other ranks (13 out of 16 or 81%). Nearly 40 per cent of respondents also thought that information technology had led to a less trusting or more paranoid organisational atmosphere (table 7.3). This opinion did not vary significantly by rank, duty or years of service.

Accountability — internal and external — was a burning issue among many focus-group participants. A familiar theme was that accountability had gone too far, and at the expense of doing the job (cf Power 1997's notion of colonisation):

> These days after Fitzgerald or what-have-you, the emphasis on accountability has become much higher, and in doing so they introduce 9321 different registers that's got to be filled out to maintain the accountability. But in doing that you spend that much time becoming accountable and spend less time doing the job you're paid for. I think accountability is a good thing, but at the same time it's got to be weighed up between getting the job done. And trusting people too, you get to the point where you're so busy being accountable you feel that

Table 7.3
Impact of information technology on accountability, management and decision making

		Per cent of respondents		
Information technology has led to …	***n***	**Strongly agree/ agree**	**Neutral**	**Disagree/ strongly disagree**
… improved police accountability.	463	63	32	5
… an overemphasis on accountability.	467	59	35	6
… a less trusting (or more paranoid) organisational atmosphere.	466	38	48	14
… improved management practices.	467	38	45	17
… increased participation in decision making at all levels.	464	21	51	29

> nobody trusts what you do … You've got to be given that trust and it be understood that you will do that job. (FG2: OICs)

Another concern was with how the information in the systems was going to be used. For example, with CRISP, if there is a complaint about inaction on a crime report, the tools are there to find the individual responsible, and to show what the person did or did not do. The concern there was whether it is about punishment or accountability — 'it's almost as if all the technology is aiding punishment as well as the accountability process' (FG5: Intel/Tacticians). Officers were also concerned that the information they enter will be accessible by FOI requests, so there is a need to teach people to be careful about the data they put in (FG5: Intel/Tacticians).

Some thought that within the Police Service there is an overemphasis on risk management, as a participant in another focus group explained:

> A lot of the issues that have been raised all relate to risk management. I feel the department has gone risk-management crazy — and you could point your finger to all the databases that belong to risk management. I know we can't get rid of them, that's a large percentage of a policeman's work. And as a police officer who was on the road, our chief thing was to try and get as much done in as least time, so we cut a lot of corners. With all these new databases we can't cut any corners … We used to go in five minutes before the end of shift, have a beer and type the running log — tap away, chat, have a few beers after work, go home. Can't do that now and it's because of risk management — over-exaggerated risk management. (FG5: Intel/Tacticians)

A participant from another group agreed, 'it's about auditing and checking … and it's overdone … it's accountability and it's gone too far … it's not being productive' (FG4: Detectives). Another officer pointed out that in some regions, an additional layer of accounting was imposed by management:

> You not only go into the computer indexes and registers, the boss then produces these A4 sheets of paper that you have to [go] through with your pen that replicates all the information and summarises it for him because he doesn't want to have to go through 12 indexes. So you've done it 13 to 14 times and then you've got another summary sheet that they want to put on the front of the QP9 and it just goes on from there. Because there's so many indexes now bosses are getting so confused and it's got to the point where auditing becomes a nightmare and to try and simplify auditing and make sense of it we've had to produce other forms. (FG4: Detectives)

Other members of the group pointed out that many of the risk management and accountability exercises are 'futile' and not worth the time. For example, 'it takes eight hours to do a station audit of tapes, and every now and then you will get one person who has forgotten to put in a tape'. Risk management should be about minimising risk, but, according to one of the participants, the Police Service's idea of

risk management is that there should be no risk, no acceptable level of risk — 'they haven't grasped the concept'. Another officer agreed:

> The idea of risk management is to identify something everyone's doing wrong, e.g. entering an index wrong — not to check every index they're doing to make sure they're doing it. It's to check problems with the system, not as an accountability exercise, which is what they're using it as. (FG4: Detectives)

Management and decision making

Just over a third of the survey respondents thought that information technology has led to improved management practices, while 17 per cent disagreed (table 7.3, p. 96). These opinions varied by rank, but not in a linear fashion — Senior Constables and Sergeants were more likely to disagree compared with other ranks: FYCs (13% disagreed), Constables (13%), Senior Constables (28%), Sergeants (22%), Senior Sergeants (11%) and Inspectors (13%; chi-square, $p < 0.05$). Length of service appeared to be a significant factor: those who had served more than 20 years in the QPS were more likely to agree that information technology had led to improved management practices (55%), compared with those who had served 11 to 20 years (35%) or 10 years or less (39%) (chi-square, $p < 0.05$).

Although some respondents (21%) agreed that information technology had increased members' participation in decision making at all levels, a larger proportion disagreed (29%). Here the percentage of respondents who disagreed increased with rank: FYCs (22% disagreed), Constables (24%), Senior Constables (38%), Sergeant (37%), Senior Sergeants (36%) and Inspectors (44%).

A recurrent theme among focus-group discussions related to the appropriateness and abuse of statistical indicators. One example cited was the use of IT-generated statistics as performance indicators — a detective's crime report might show that he has 30 files, but it doesn't show the six coroners' files he has got to investigate, which could be quite substantial, and it may not show the interstate offences he is investigating (FG4: Detectives). Another example was the use of CAD statistics for resource allocation. A general duties officer in one focus group explained that in one area of inner Brisbane a lot of jobs are 'on the fly' (offenders caught in the act) and do not always get entered on CAD, so their CAD statistics did not compare favourably with other areas. This officer went on to give another example where officers in a watchhouse abused the system by putting in a job every time they feed a prisoner, so that they get a job number from CAD each time. Similarly, it was claimed that an officer can arrest someone with 100 warrants and enter the data for each arrest on each warrant to show how busy he has been (FG1: GDs). Another bone of contention was clear-up rates. Detectives blamed CRISP data entry operators for not recording all their clear-ups, while others were concerned that monthly fluctuations in clear-up rates might give misleading indicators of performance (FG2: OICs):

> With clear ups, if you pick three months, say, January, February and March, one of the big chiefs … might look at February's clear-ups and there might be one per cent in break and enters, say. In actual fact there's been … 80 to 90 offences cleared for that month. What you've really got to do, because they're two months behind [is to] wait till April or May and then go back to February, because your clear-up goes back to the month in which the offence was committed, it doesn't go to the month when it was actually cleared up. So the boss might say to you, 'gee, your clear-up rate for Feb. is poor', and you've actually got to say, 'hang on, boss, give me a ring back in May and we'll see what it's like then' … the boss is kicking you in the backside. (FG2: OICs)

Cultural conflict

The introduction of information technology appears to have created new cultural conflicts and reinforced old ones within the organisation.

Operational culture v. information technology culture

Some of the discussion in the focus groups reflected a sense of alienation and distance between police and information technology personnel (FG2: OICs), the perception for some being that IT developers were there to 'support their own work', and had little understanding of the technology needs of police (FG1: GDs; FG2: OICs). Indeed, individuals who perceived that they had not been consulted in system design spoke in terms of this distance between two worlds: that the 'consultancy mobs' come in and 'hear what they want to hear' (FG5: Intel/Tacticians), or that sometimes ideas are generated from above and 'we end up getting the wrong answer' (FG7: OICs; FG4: Detectives).

For some, the non-operational services represented a challenge to the status of the operational police officer and a loss of direction in terms of the Service's core business:

> Ten years ago, the operational police officer was the nucleus and everything was ancillary to that … we've just been turned inside out. We're on the outside and the ancillary divisions are now on the inside. It's like we're supporting them, but they really should be supporting us … (FG6: GDs)

> I always had the view that people in other areas, support service or whatever, were supposed to facilitate the work of what is our core business. It seems to me the other way round because people and groups come up with you-beaut ideas and schemes and say 'you will make it work'. We either make it work or we find out it doesn't work then someone else will change it and move on and we either don't do it any more or someone else comes up with another idea. There's no consultation. (FG5: Intel/Tacticians)

Cultural divisions were also evident in the discussion of inadequate resources in one group, where some said that the systems were designed using powerful computers, yet at the users' end the resources were not there to support the systems (FG5: Intel/Tacticians). Others were, however, more sensitive to the limitations faced by the information technology developers, in terms of both resource (FG10: District Officers) and policy constraints (FG2: OICs).

Central v. local

The cultural division between central administration and local operations was epitomised by attitudes to so-called rogue (bootleg) systems. The advantages of locally developed, stand-alone systems are that they can be up and running in a short time, enabling police to meet their immediate information management needs (FG8: RIMOs), that they circumvent the slow bureaucratic process which was perceived as impeding development at times (FG11: Chief Superintendents), and that they help to meet immediate information technology requirements imposed by legislative demands (FG9: Specialist Investigators). The disadvantages of these systems are that they create security problems (FG8: RIMOs) and result in a lack of integration and standardisation within and between regions (FG8: RIMOs). While rogue systems can be up and running quickly, they can die just as quickly, either because the 'champion' of the project leaves, or, in some cases, they can be 'choked' (FG8: RIMOs). Participants in one focus group acknowledged the skills of those who design these systems, and their awareness of user needs, and suggested that these systems should be harnessed — 'combining the best of what's around' (FG7: OICs).

Participants in some group discussions were also critical of the 'blue ties' in headquarters who, they felt, were out of touch with operational police needs and realities (FG2: OICs; FG1: GDs; FG5: Intel/Tacticians). It was suggested that many initiatives (not just information technology) were about 'careerism' (FG1: GDs) and empire building (FG2: OICs), with rivalry and bitterness between groups (FG5: Intel/Tacticians). As a result, police on the street suffered (FG1: GDs).

Police v. civilians

Another cultural division exacerbated by information technology was that between police and civilians. This was evident in focus-group discussions on practical and technical problems in connection with information technology. One group complained that civilians had more powerful computers than police (FG9: Specialist Investigators), and most groups agreed that staff in headquarters were much better equipped than operational police.

Some of the problems with CRISP data entry and communications (see chapter 5) were attributed to the fact that the information was being entered or relayed by civilians who 'have no idea' about police work (FG1: GDs). Police complained that

CRISP operators were not trained in legislation (FG4: Detectives), did not understand the policing process (FG3: OICs), and were inadequately trained in offence definitions (FG2: OICs). Because many information technology workers are civilian, this division is also related to the cultural conflict between police and information technology workers. Cynical remarks were made by police, such as information technology planners were 'public servants try[ing] to tell us what's good for us' (FG4: Detectives), or information technology support was not always available out of hours because 'public servants work 8 to 4 Monday to Friday, [whereas] the system goes down outside those times, during the busiest times, when you're dealing with angry pissed men' (FG1: GDs).

Sworn officers appeared to feel threatened by the trend towards 'civilianisation' of the police organisation. In one focus group, civilianisation was seen as debasing the value of police. One participant said that, when the administration took an officer off a job, he was replaced with three public servants to do that one job. One example cited was the fact that there were now four public servants in the equipment office where there used to be just one police officer and one public servant (FG1: GDs).

Civilians were, however, also seen to have their place. They were seen as useful when they freed police up to get on with their 'operational work' (FG6: OICs). For example, it was suggested that they preferred research officers to be civilians (FG10: District Officers), and that it should be civilians, not police, doing the data entry at station level (FG6: GDs).

Management v. operational police

The division between 'management cop' culture and 'street cop' culture is a well-known phenomenon in police organisation (Reuiss and Ianni 1983). This division has been made more acute with the introduction of information technology. The perception that headquarters staff were given superior computer resources to operational police has already been mentioned (FG1: GDs; FG5: Intel/Tacticians; FG8: RIMOs). Some officers complained that senior managers did not understand that technology-based information management is resource-intensive (FG5: Intel/ Tacticians; FG8: RIMOs).

One area of conflict was differing perceptions of how the technology should be routinely used. As pointed out earlier, there was some frustration with the way managers had added to the workload of subordinates: even though information was available on databases, 'bosses' continued to ask for hard copy summaries (FG4: Detectives). According to one group, information was transcribed from the patrol logs to the occurrence sheets, yet 'the indexes are there, so it is possible for whoever it is in senior management who wants to review any particular part of the log to get his staff officer to do it' (FG6: GDs). The practice of manual record keeping

for supervisors in addition to electronic data entry was also noted in our field observation. For every call for service and ARI activated, there were two handwritten records: the officer's notebook, and a log of daily activities for the supervisor. Our observer noted that these reports were extensive and took quite a long time to complete (Observation Report 1).

As one participant pointed out, managers often asked subordinates to access databases on their behalf:

> Now the bosses won't, say, … query the index, give it a date, and punch in the ARI, the location code, it gives him the number, … but instead they'll go [sound of knocking, then in a gruff voice] 'Yeah, how many ARIs you done this week?', and the poor old boss goes … and he has to find the information and bring it back to the senior person and say … whatever the number happens to be, and the problem is that information was sitting on that other person's desk right in front of them, they just didn't want to go and use a couple of fingers, … they ring up, get other people to do the running around. (FG6: GDs)

Even a Chief Superintendent was mystified by this process:

> The question is, if we have the information here centrally, why aren't the reports generated centrally? If the data exist, why do we have to continually go down to the OICs to produce the reports in many, many instances? [Q: is there any process that would enable that to be changed?] There must be, because why bother with information technology? (FG11: Chief Superintendents)

Some participants attributed this problem to senior management's confusion with the number of indexes they need to access (FG4: Detectives) and their lack of understanding of the time it takes to respond to these requests (FG6: GDs). Others disagreed, since even computer-literate young Inspectors continued to 'pass the task down the line' instead of asking their staff to do the queries (FG6: GDs).

Relations with external agencies

As described in chapter 4, the QPS routinely provides information to external agencies, both public and private. The QPS is also closely monitored by the CJC, which is also responsible for overseeing or directly conducting investigations of police misconduct.

Table 7.4 provides examples of the type and volume of requests for criminal history checks from external organisations in 1997. It is likely that the number of requests received has increased substantially since then because a growing number of government agencies are now using criminal history checks as part of their employment vetting processes. For example, different sections of the new *Commission for Children and Young People Act 2000* are being implemented between May 2001 and

February 2002, which will require all employees and voluntary workers who will be working with children to be subjected to criminal history checks.

Officers in the focus groups showed great resentment towards these demands for information and accountability from external organisations. It was said in one focus group (FG1: GDs) that a lot of police work is for the CJC, insurance companies, security companies and other 'vested interests'. For example, the accident form is a very long form that has to be filled out by the police for every accident. Insurance companies pay the Police Service for this service and would sometimes ring to challenge facts entered on the form, which infuriated some officers:

> It pisses me off how they ring you up and they doubt what you put on the form, and you say 'mate, look, what purpose would it have served me to tell a lie on this thing, when I don't know either party and I'm an independent person?'. (FG1: GDs)

Officers also thought that private security companies used police to do their work for them. It was said that when an alarm goes off, the security people ring the police and request a car to check the premises, 'they don't even bother sending a guard out and they bill the client, and we aren't charging the security company'. Similarly, there

Table 7.4
Criminal history checks requested from external organisations
21 April – 2 May 1997

Organisation	Number of requests
Ambulance Qld	4
Consumer Affairs	12
Corps of Commissionaires	2
Emergency Services	2
Family, Youth and Community Care	34
Police Headquarters Security	6
Health	5
Intellectually Disabled Citizens Council	2
Register for Justices of the Peace	3
Jury Panels	2
Liquor Licensing	10
Machine Gaming	1
Mines and Energy	1
Principal Club	1
Prosecutions, Commonwealth Government	3
Scout Association	1
TAB	2
Transport	2
WorkCover Qld	2
Corrective Services	4
Gold Coast Homeless	2
Total	**101**

Source: IMD Client Survey and Service Quality Report, June 1997, p. 36.

were concerns that the CJC has imposed a variety of reporting requirements that make officers' work more cumbersome.

One manager questioned the wisdom of this trend to service external demands for information:

> We've gone away from our core business … with the information we're capturing for other people … it's costing money to store it, it's costing money to maintain it, costing money to do quality checks — who's using it, what are they looking for, who needs it? (Interviewee #6)

Another Information Technology Manager thought that police could make better use of the data they have collected: ' … we are tremendous collectors of information and in some ways not good users … ' (Interview #10).

Summary

Information technology, according to police who participated in this study, has had a positive impact on workplace relations: it has led to improved information sharing between workers and improved communication, and has facilitated teamwork. On the other hand, information technology has led to closer scrutiny of police work by supervisors and has made supervisors more aware of the day-to-day activities and workload of officers under their command. This increased awareness of work activities by supervisors was perceived most frequently by detectives, who traditionally enjoyed a great degree of autonomy and freedom in their daily activities. There was general agreement that, with the introduction of technology, police were required to report on their activities more frequently. Senior officers, most of whom have managing or supervisory responsibilities, reported that information technology has meant that they spend more time on paperwork, planning and checking the work of their staff for 'compliance'. However, the capacity provided by technology for checking has not been fully explored by supervisors because they 'didn't have time'.

Nevertheless, the majority of police thought that information technology had led to improved police accountability, although they also thought that it had led to an overemphasis on accountability. Officers were concerned that accountability requirements had increased at the expense of 'core' police work, while the organisation had gone 'risk-management crazy'. Some felt that the amount of auditing and checking had gone too far and had become counterproductive.

While a majority (over 50%) of senior officers at the rank of Inspectors and those with more than 20 years of service at the QPS thought that information technology had led to improved management practices, more junior and less experienced officers were less likely to agree. There was also little support for the proposition that information

technology had increased participation in decision making. Officers in focus groups were concerned that statistical indicators could be misleading or abused.

Information technology also appears to have reinforced old cultural conflicts between central administration and local operations, between sworn officers and civilians, and between management police and operational police. It has also created new divisions between operational police and information technology personnel. The perception among operational police was that central administration, civilians, management and information technology staff did not understand operational policing needs, and were more concerned with their own careers and 'empire building'. Operational police also resented what they saw as an inequitable distribution of resources: their perception was that, while they had to live with outdated and inadequate computer equipment, civilians and headquarters staff were given more and better computer resources.

With the advent of information technology, the QPS has become a supplier of information for a large number of external agencies, including government departments, private companies and individual citizens. This has created a great deal of resentment among operational officers who felt that these demands were placing an increased burden on officers and detracting from the core business of policing.

Chapter 8: Conclusion

As stated in chapter 1, this research project was designed to assess the impact of information technology on policing. It aimed to address questions such as: How has information technology been received by police? Has this technology changed police practices at operational or management levels? What impact does technology have on the structural conditions and cultural assumptions of policing? Can information technology be a useful tool for police reform?

In this concluding chapter, we summarise the answers to these questions as indicated by our research findings, and discuss their theoretical and policy implications.

Information technology in the QPS

The QPS provides a theoretically significant case study in which major technological change and organisational reform have occurred over the same period of time and have become intertwined. As detailed in chapter 4, the development of information technology in the QPS was driven by a number of technological, managerial and policy concerns. The introduction of computer technology in the mid-1970s was modest and haphazard, being directed at responding to the information needs of a specific crime problem (vehicle theft). With the advance of information technology, the use of computer systems was expanded over the next two decades to include processing of data for crime recording and investigation, communication with other government agencies, and computer-aided dispatching. Successive attempts to upgrade the information systems were made to redress technical deficiencies found by various external inquiries — quality of data, accessibility, lack of integration and various inefficiencies.

By the late 1980s, however, several sources of external pressure had accelerated the push for new and better information technology. The Fitzgerald Commission of

Inquiry, apart from uncovering serious corruption, was critical of the police force's reactive policing style and rigidly hierarchical management structure. In its final report (Fitzgerald 1989), the Commission of Inquiry recommended major reforms to bring about a shift to a community-based, problem-oriented style of policing, as well as more flexible and efficient management practices. The Commission also recommended a comprehensive review of QPS information systems to improve the organisation's management capacity.

The subsequent establishment of the CJC as the agency responsible for monitoring and reviewing the implementation of police reform in the QPS brought with it additional demands for information for accountability purposes. Accountability requirements of new legislation have also markedly increased the pressure on the QPS to improve its capacity to collect, store and retrieve information. At the same time, the organisation has had to cope with the rising tide of demand for information from a variety of external government and non-government agencies.

The QPS's transition from a low-technology organisation in the early 1980s to the current state of high technology has not been an easy one. Organisationally, the QPS was totally 'immature' in the early 1990s, not only in relation to information technology, but, more significantly, 'there was really no management infrastructure to speak of at all', following the removal of top levels of management as a result of the Fitzgerald Inquiry (Senior Information Technology Manager, Interview #12). The architects of the information system followed a deliberate strategy of initially securing support for and ownership of the system among operational police, before focusing on managers. The idea was to move gradually from an ad hoc, operationally oriented system to an integrated, tactical, strategic and eventually policy-oriented system (Senior Information Technology Manager, Interview #1).

Acceptance of technology

Our data showed that by the late 1990s information technology had become well accepted and widely used by police in the QPS. Systems such as CRISP were used by 80 per cent of the survey respondents every day or several times a week. The vast majority of respondents thought that technology had made a great difference to police work. This feeling was particularly prevalent among respondents who have had longer service in the QPS and those in higher ranks. In spite of many complaints in the focus groups about various technical problems (see chapter 6), QPS officers' assessment of the impact of technology on their own work was generally positive. The majority of survey respondents indicated that information technology has allowed them to work more effectively, made their work easier and helped them cope with the amount of information police need to do their work properly. The perception

of gain in efficiency as a result of information technology was especially strong among police who had experienced the old technology.

Survey respondents also rated positively the impact of information technology on workplace relations and communication. The majority agreed that information technology has led to improved information sharing and improved communication between workers. Similarly, respondents tended to agree that information technology has allowed people to work more cooperatively and created a more positive work atmosphere. Improvement in communication between workers was largely the result of the availability of e-mail which facilitated teamwork, information gathering and information sharing. Information technology was also perceived to have had a favourable impact on the quality of police service. Six out of 10 survey respondents thought that information technology has led to improved police service to the public and improved police response to crime. Several focus groups mentioned that the crime-reporting system has made police procedures more transparent and has allowed victims and complainants to get faster feedback on the progress of their cases. Our observations also found enthusiastic support from operational police for the mobile data facility that gave police direct access to data on outstanding warrants (see chapter 5).

Impact on police practices and performance

Information technology has the potential to change and improve police practices and performance in various ways. For example, computer-aided dispatch systems can be used to better manage the deployment of police vehicles and make police patrol activities more information-driven. The capability of these systems can be further enhanced by the use of global positioning systems (now widely employed in the taxi industry, among others) that provide accurate, real-time information about the location of vehicles. Well-designed information systems can also facilitate the apprehension and detection of offenders by increasing the range and timeliness of information that investigators can access, by providing analytical tools that can be used to profile suspects and identify offending patterns, and by making it easier to identify and track repeat offenders. In addition, information technology can substantially assist problem-oriented policing activities by aiding in the identification of problem areas and addresses, by highlighting trends and patterns that warrant attention by police and other agencies and by allowing information to be shared by agencies (Abt Associates 2000).

Although the scope for information technology to enhance police effectiveness is considerable, our research and the findings of other reviews (Queensland Police Service Review 1996; CJC 1998b; CJC forthcoming) indicate that this potential has yet to be realised in the Queensland context. In most areas of the State it would appear

that random — rather than intelligence-driven — patrolling continues to be the norm. Clearance rates have not shown any significant improvement over the last decade, suggesting that the investment in information technology has not, to date, resulted in the police becoming measurably more effective in catching offenders and solving crimes. Recent efforts by the QPS to promote the concept of problem-oriented policing (POP), by such means as preparing and promoting manuals and providing funding support to new projects, have also met with only limited success to date.

Our overall assessment is that information technology has enabled police to do some existing tasks better and more efficiently — such as record and gain access to offence details, enforce warrants and run criminal history checks — but has not yet led to major changes in how the QPS deals with crime and disorder issues. This was also the view of many of the officers who we surveyed: fewer than 40 per cent thought that the new technology has led to a more problem-oriented police service or better proactive policing. Some officers in one focus group mentioned the potential for 'intelligence-driven patrols', 'hot spots' and repeat-offender analysis, and proactive crime investigations, but others were sceptical of the prospects for successful implementation As one focus-group participant pointed out, IT may have given police the potential to be more proactive, but they lack the necessary resources and expertise to realise this potential.

To some extent, efforts to make the QPS more information-driven have been hampered by shortcomings in the technical systems themselves: key databases such as CRISP and CAD are not linked; some important types of data (such as call histories for addresses and repeat victimisation profiles) cannot be readily accessed; output is difficult to interpret because of the lack of standardised, user-friendly, reporting functions; and managers cannot readily access timely data on trends and patterns at the local level. These shortcomings are, in turn, partly attributable to the poor state of QPS information technology systems in the early 1990s, which meant that priority had to be given to establishing a basic computing infrastructure and the core systems such as CRISP and Polaris, rather than to addressing higher-order issues such as database linking and the development of management information systems. However, the barriers have not simply been technical in nature. Arguably, had there been a stronger commitment within the QPS from an earlier stage to promoting more innovative forms of policing, there would have been more demands placed on the information technology area — from above and below — to develop appropriate technical systems to facilitate these innovations.

In this regard, an important obstacle has been the dominant 'technological frame' of policing, which has tended to see information as useful only if it leads to arrests. According to one interviewee, information technology has, in effect, 'made things easier, rather than made things different', because of the lack of an alternative model of policing.

> … even our 'intel' people, even the high-end users, our power users, generally see information from an offender perspective — in other words, information analysis is all about how we can … find an offender … how do you nick someone, and so that limits what becomes useful information. (Senior Information Technology Manager, Interview #1)

The broader political climate in Queensland has also tended to insulate the QPS from the pressures now being experienced by police agencies in some other jurisdictions. The Service has not yet had specific crime reduction targets imposed on it by government. Similarly, local, district and regional managers have not, to date, been required to achieve any firm performance targets in terms of crime reduction or problem solving; nor have there been effective systems in place for monitoring and comparing the performance of different areas of the Service (CJC forthcoming). Instead, there appears to have been a political consensus in Queensland that what matters most to the electorate are issues such as police numbers, the number and location of 24-hour police stations, police visibility and response times. If anything, changing established policing methods has been seen as a high-risk strategy because of the political sensitivities associated with issues such as response times, police visibility and the like. For example, a trial of negotiated response strategies on the Gold Coast in 1997 was quickly aborted after the fact that police would not be attending every call from the public became a political issue: see CJC 1997c. Another consequence of the preoccupation with political issues such as police numbers and visibility has been that most of the additional funding provided to the QPS in recent years has been to pay for additional police rather than new technical infrastructure.

As at mid-2001, the QPS was implementing a performance monitoring framework that will be used as a basis for regularly assessing districts' effectiveness in dealing with crime. Through the budget process, the Queensland Government is also gradually increasing the performance reporting requirements for the QPS (and other public sector agencies). Other Australian police services — such as the New South Wales and South Australian Police Services — have also begun to adopt a more proactive approach to tackling crime and disorder problems, ostensibly with some success, which has provided the QPS with useful models to follow. However, it is too early to determine the extent to which these recent internal and external developments will result in significant changes 'on the ground' in how the QPS addresses crime and disorder issues. As other studies have shown, it is very difficult for policing organisations to move from a narrow focus on delivering reactive policing and catching offenders to a broader focus on problems, even in circumstances where there is strong commitment at the top to implementing such a shift (see, for example, Sparrow 1991, Abt Associates 2000).

Information technology and accountability

As discussed in chapter 4, the impetus for the maintenance and upgrading of information technology in the QPS has come, in part, from new management and accountability requirements. In recent years the QPS, like many other policing organisations, has begun to impose a broader range of accountability controls, often in response to externally generated requirements. For example, new police powers legislation in 1997 and 2000 created substantial additional recording requirements in relation to the conduct of searches, the detention of suspects for questioning, the use of move-on powers, DNA testing, the diversion of minor cannabis offenders, and so on. The Service is also implementing comprehensive recording requirements for personal searches in response to recommendations contained in a recent CJC report on police strip-searching practices (CJC 2000a). In addition, the QPS, as part of its own risk-management processes, is expanding the range of information being recorded about police activities (such as police vehicle pursuits, complaints, use of capsicum spray and injuries to officers).

The police officers in our study saw a close association between greater use of IT by the QPS and the increased emphasis on accountability. Two-thirds of the survey respondents agreed that information technology has required them to report on their activities more frequently and has made them more accountable for their actions — although a number of focus-group participants pointed out that it was the need for accountability that caused the additional workload, not the information technology systems *per se*. Just over half of the survey respondents thought that information technology has led to a closer scrutiny of their work by their supervisors and has made their supervisors more aware of their day-to-day activities and workload. Information technology was also seen as having put constraints on police discretion in some areas. About a quarter of survey respondents thought that technology has restricted their discretion, particularly in relation to taking shortcuts in processing cases. A fair proportion (43%) also thought that technology has required police to follow unnecessary steps to get things done. This feeling was particularly strong among detectives and officers in the higher ranks.

Although officers frequently complained that risk management and accountability have gone too far, it is possible that they have overstated the extent to which their behaviour is now subject to closer scrutiny. Some local bootleg systems have been developed to record information about the workloads and performance of individual officers, but this is not being done on a Service-wide basis. The CRISP and CAD systems provide a record of officers' actions (or inactions), which can assist in investigation of complaints and monitoring of work performance. However, it was evident from focus groups with supervisors that the monitoring capabilities of these systems were generally not being used — the main explanation offered by

supervisors was that they were too busy. The ESC is now using complaints data to profile officers and work units with excessive complaints histories and to monitor trends, but the report-generating capabilities of the system are very limited and it is not linked to other internal databases (such as personnel records) or to the complaints database held by the CJC. Other databases, such as the Custody Index (which records details about the exercise of a range of police powers) are very difficult for supervisors to access and interpret.

In some respects, information technology has actually been a source of new accountability risks. Police organisations hold, or have access to, information for which there is a strong, and growing, external demand (such as details on criminal histories, motor registration and address details). The creation of computerised databases that can be directly accessed by large numbers of police has increased the opportunities and incentives for police officers to provide such information to unauthorised parties. For example, a recent CJC inquiry into unauthorised release of confidential information by police (CJC 2000b) identified one case where a considerable number of officers at a regional police station had unlawfully disclosed confidential information to a private investigator who also worked at the station as a cleaner. In another instance, an officer had routinely used the QPS database to help him to locate debtors on behalf of a debt recovery agency. As of November 2000, 13 officers had been disciplined or had resigned as a result of investigations carried out for the inquiry (CJC 2001a). In addressing these and other risks, there has been an ongoing tension between QPS operational priorities on the one hand and the CJC's focus on accountability issues on the other. In particular, the QPS has expressed concern about the costs and adverse effects on operational efficiency of imposing additional controls on officers' access to databases (CJC 2000b). Similar arguments have been advanced by the Service for not moving more quickly to implement some key recommendations of a major internal review ('Project Alchemy') that related to procedures for recording details about confiscated drugs and other high risk property such as cash (see CJC, Police and Drugs 1997a).

In summary, police are now being required to record more information for accountability purposes and officers feel that they are under more scrutiny. On the other hand, managers are making only limited use of information technology systems for monitoring purposes, the systems themselves have a number of shortcomings and, in some areas, risks may have actually increased as a result of the greater ease of access that officers have to confidential information. Consequently, the extent to which there has been a net increase in accountability as a result of the increasing use of information technology is very difficult to determine at this stage.

The paperwork issue

Police agencies, like other large bureaucracies, are still very paper-intensive organisations in which a great deal of time is spent on completing reports, and considerable organisational resources are expended on administering paper flows and storing and maintaining records. 'Too much paperwork' has been a common complaint by police and is often cited by them as an explanation for why they are unable to spend more time on policing tasks such as conducting patrols and investigating crimes. As noted above, managers and supervisors also frequently give this as a reason for not taking a more proactive approach to the enforcement of accountability requirements.

Information technology has often been held out as providing a solution to the paperwork problem in policing and other bureaucracies by streamlining administrative processes (such as by eliminating the need for multiple forms and multiple entry of data), by making information easier to retrieve and by reducing the number of hard copy records that must be generated and maintained by organisations. However, some studies have raised doubts about whether information technology has, in fact, led to net gains in this regard, at least in the context of policing. For example, Ericson and Haggerty (1997) reported that unintended consequences of the introduction of information technology into the police departments that they had studied were an increase rather than a decrease in paper files, and police work becoming even more office-bound in some cases.

Many of the QPS officers surveyed for this study said that, as a result of information technology, they now spent more time dealing with paperwork. Respondents in the survey reported spending an average of 3 hours and 37 minutes per 8-hour shift using computers for administrative tasks. Although there are no baseline data from a previous period for comparison, the perception of 4 in 10 survey respondents and many focus-group participants was that the new technology has led to officers spending less time on the street.

While some processes in the QPS (for example, for recording calls for service information) are now fully computerised, there is, as yet, no capacity for mobile data entry. As a consequence, operational police still have to rely heavily on printed forms for the initial capture of information. In addition, because key electronic indexes and registers are not linked, the same information often has to be entered multiple times, which many police understandably find very frustrating. The Polaris project is meant to provide a long-term solution to this problem, but, as discussed in chapter 3, there have been significant delays in implementing key elements of this project, which, in turn, have led to growing cynicism within the QPS about whether Polaris will ever deliver on the promise of single entry of data.

Respondents' complaints about the growing paperwork and administrative burden need, of course, to be placed in perspective. A fair number of these officers occupied supervisory roles that, by their nature, required them to devote more time to administration and less to operational police work. It is possible that some of these officers may have had difficulty distinguishing between the impact of information technology and the effect of changes in their own role within the organisation. There also may have been a tendency, especially for older officers, to look back to a non-existent golden era of paper-free policing. The historical evidence from Queensland and other jurisdictions strongly suggests that complaints about police being office-bound hardly amount to a recent phenomenon. A 1969 review of the Queensland Police Force, undertaken by the then South Australian Police Commissioner, Brigadier McKinna, described in very critical terms a highly routinised organisation in which large amounts of time were spent typing numerous reports and rosters, and in which disproportionate numbers of officers were assigned to doing what was essentially clerical work (Queensland Police Service Review 1996 pp. 17–20). Similarly, a 1988 review of operational work practices by Arthur Andersen and Company highlighted the volume of police time wasted on typing forms (Queensland Police Service Review 1996, pp. 23–4). Without comparable historical data, we simply do not know whether officers are now more immersed in administration and paperwork than they were prior to the introduction of information technology. Nevertheless, it is certainly the case that the amount of time being spent on such tasks remains substantial and that the much-touted potential of information technology to streamline administrative processes has yet to be realised.

Factors that have prevented the paperwork burden from being reduced in the QPS include: limited capability of information technology systems themselves, the need for information technology managers to balance competing priorities, and the growing emphasis on accountability in its various forms. Information technology may well have the potential over the longer term to deliver substantial administrative efficiencies for police organisations by eliminating duplication of paper and electronic records and multiple entry of the same data. However, whether this will result in police officers spending less time on paperwork (broadly defined) and more on the street remains to be seen.

One consequence of making it easier for police to collect and process information is also to make it easier for managers and policy makers to request that more information be recorded. Hence, any gains in the ease with which specific recording and administrative requirements can be complied with may be counterbalanced by an increase in the sum total of requirements. It also cannot be assumed that officers will necessarily become more productive once they have less paperwork to deal with: if the time saved is spent in engaging in more conversations with colleagues in the police station, or in conducting additional unstructured mobile patrols, there may be

no net increase in policing effectiveness. As we argue below, the ability of the QPS and other police organisations to reap the benefits from information technology will depend heavily on their having the right organisational settings to use this technology effectively.

Police culture

Information technology has created a new form of 'cultural capital' (considered to be a valuable resource in policing) and has also imposed new constraints on police work. Technology has redefined the knowledge and skills required for doing police work. Information, always a valuable commodity in policing, must now be entered, stored and retrieved in a way dictated by the technology. Policing knowledge, which used to be carried inside police officers' heads, has now become synonymous with data, which is too complex and too voluminous for the human brain to cope with. Officers, especially those in junior operational positions, need to acquire computer skills simply to get their work done. This means that their daily work has become dependent on technology: whether they are able to complete a report, retrieve a piece of information, or get out of the station now depends on whether they have access to a computer, whether the system is down, whether the computer is powerful enough and whether they have the skills to use the technology. Thus, information technology has become accepted in the QPS as a necessary resource for policing and technical (information technology) expertise has become a much-valued form of cultural capital. As one intelligence officer explained:

> As intel officers we were considered the leaders in information technology. We knew nothing, but we knew so much more than the basic [officer] who knew practically nothing. We were gods to them. (FG5: Intel/Tacticians)

The growth in funding and staffing of IT-related functions within the QPS was a source of much envy and some bitterness among some officers. The ascendancy of officers with information technology expertise may also have threatened the traditional power structure of an organisation where previously leaders were predominantly drawn from the criminal investigation branch (Interview #1). The embrace of the new technology was nevertheless accompanied by an acute awareness of its constraints — information technology was seen to have imposed new limits and generated additional work for police, as discussed earlier.

Although information technology skills are highly valued, some officers were not entirely comfortable with the increased reliance by police on technology for information. They felt that reliance on information technology has meant the loss of local knowledge and the decline of hands-on intelligence gathering.

As described in chapter 7, information technology has created new cultural divisions and reinforced old ones within the police organisation. One traditional division that has survived, however, is that between management and operational police. Six out of 10 respondents agreed that IT has led to an overemphasis on accountability. Nearly 4 in 10 also thought that technology has led to a less trusting or more paranoid organisational atmosphere. A familiar theme among focus-group discussions was that accountability has gone too far and often at the expense of 'doing the job'. Some officers felt that the Police Service had gone 'risk-management crazy'. They thought that all the auditing and checking was overdone and counterproductive. Some were also concerned with the abuse of technology-generated performance indicators.

Another cultural value not challenged by the new technology is the longstanding resentment that many operational police have against external scrutiny. If anything, this resentment has been justified as information technology has led to the proliferation of indexes and registers police have to fill out as part of legislative or other accountability requirements. Officers complained that these reporting requirements have made police work more cumbersome.

Our conclusion, therefore, is that information technology has transformed the structural conditions of policing in the QPS in some important ways, while leaving many cultural assumptions and traditional policing practices unchallenged.

Implications for police reform

This study has shed light on the scope for — and barriers to — using information technology as a means of enhancing police effectiveness. The experience of the QPS, while unique in some respects, illustrates the more general point that giving police access to computers, increasing the range and quantity of information that is stored electronically and automating what were previously manual processes will not necessarily increase organisational effectiveness or change how the business of policing is conducted by the agency. As Manning (1992a, p. 350) has argued, the traditional structure and culture of policing are, in many respects, significant brakes on the capacity of police organisations to use information technology to enhance their effectiveness. If police agencies are to get a better return on their investment in IT, there must be a conscious and sustained effort to change the organisational settings in which that technology is introduced. Effective implementation of intelligence-driven patrolling, for example, requires not only information systems that can provide data on hot spots and hot times, but also analysts capable of interpreting this information and, most importantly, work-allocation systems that deploy patrols accordingly. A similar conclusion was reached in a recent American report on the use of information technology to support community and problem-oriented policing.

> Community and problem-oriented policing will require that police agencies 'act smarter' in the future, in that information about problems, events and situations will form the basis for designing effective police interventions. Technology alone, however, cannot replace a well-designed and departmentally integrated COPS or POP strategy. Without a system of COP/POP in place in a department, the acquisition of technology, in any of its manifestations, is a potentially empty experience. (Abt Associates 2000, p. 154)

While enhanced information technology may not, of itself, be sufficient to change policing practices, inappropriate technology can often act as a barrier to change. As various studies (Sparrow 1991; Abt Associates 2000) have shown, there is often a considerable disjunction between the information technology that agencies already have and what they need to support the use of more proactive policing strategies. In the case of the QPS, for instance, the CAD system that was developed in the early 1990s has been very useful for managing traditional reactive policing activities, by making it easier to deploy vehicles, monitoring of work volumes and response times, and so on. However, the current design of the system makes it very difficult to use the stored data to identify problem areas and addresses, which has been, in turn, one of several barriers to promoting the greater use of problem-oriented policing within the QPS.

An important lesson from this case study is that the focus of planning for information technology needs to be on assisting organisations to get where they should be, rather than simply on streamlining — and thereby entrenching — established practices. This, in turn, requires that policing organisations articulate clearly the management and work practices that they are seeking to implement. Secondly, they must have structures for ensuring that IT planning decisions take these requirements into account. Thirdly, and most importantly, they must commit to implementing organisational changes on the ground to promote the more effective use of information.

Implications for theory of technological change

The research findings presented in this report were generally consistent with Ericson and Haggerty's (1997) conclusion that information technology has altered some important aspects of the structural conditions of policing. In the case of the QPS, within a relatively short time after its introduction, information technology has redefined the value of communicative and technical resources, institutionalised accountability through built-in formats and procedures of reporting, and restructured the daily routines of operational policing. Information technology has also allowed police procedures to be more transparent to the public, and this transparency has become accepted as an indicator of good police service. Similarly,

officers are beginning to appreciate the value of using technology-generated information for tactical and strategic purposes such as crime prevention, problem solving and resource allocation. Nevertheless, technology has left unchallenged many cultural assumptions of policing. Most notably, the dominance of traditional policing styles and values has not changed substantially. Although information technology has given police the capacity to employ a 'smarter' or problem-oriented style of policing, this capacity has not been fully used. Even where technology has aided proactive police work, such as the checking of outstanding warrants, it has been used mainly to support a traditional law-enforcement style of policing focused on clear-up rates. Cultural suspicion and cynicism against management and external watchdogs are also still very much alive, although these feelings have now been channelled into hostility towards the organisation's perceived obsession with risk management and to external agencies' demands for data and accountability.

The case study sheds new light on the role of cultural factors in understanding the impact of technological change. There was undoubtedly a clash in 'technological frames' (Orlikowski and Gash 1994) between the users and the architects of the systems. Users of the technology, even the more advanced ones, expected it to make their work easier and more efficient, without their having to change existing policing and management styles. Architects of the systems, on the other hand, have intended the organisation to move towards a more sophisticated mode of information usage — for resource management, strategic planning and policy decisions. At the same time, governments and other external bodies have continually demanded that new legislative and accountability requirements be incorporated into the design, so that the capacity and functionality of the systems have had to be constantly expanded. Yet the case study showed that users' technological frames are not immutable. While police resent the additional workload generated by managerial and accountability demands, they have also become willing players in the new technological game. The coercive nature of the technology gave them no other alternatives. Thus, despite constant complaints about various technical problems, police have generally responded well to the new technology. Ironically, rather than resisting the burden imposed by the technology, they demand more and better of it in the hope of lightening this burden. If Orlikowski (1996) is correct in saying that organisational change is likely to be emergent and continuous rather than rapid and discontinuous, technology-based organisational change, by gradually and continuously altering the structural conditions of policing, will eventually have an impact on the deeply embedded assumptions of police practice.

Appendix: Timeline for the introduction of IT systems to the QPS, 1994–2000

1994–95

- Pilot system of CRISP (which replaced the Criminal Offences Index) in the Metropolitan South Region.
- Commencement of CRISP in South Eastern and Metropolitan North Regions and State Crime Operations and Operations Support Commands, March to June 1994.
- Statewide implementation of CRISP by December 1994.
- Upgrade of computer mainframe to handle the increasing demands of CRISP and other QPS systems, May–September 1994.
- Special $10 million funding for enhanced information technology (mainly spent on CRISP).
- A further $30 million allocated over three years (1994–97) to fund the initial implementation of infrastructure and integrated systems.
- Establishment of a statewide computerised offender identification system (Com-Fit).
- Pilot of new network system in Ipswich District, April–May 1994 (3-Com routers and Netcomm modems).
- Statewide implementation of new network, 30 November 1994.
- Evaluation of tenders, implementation and training of a new relational database and applications environment.
- Tenders called for the provision of a corporate e-mail system.

- Purchase of 600 workstations and 200 laser printers.
- Development of the Transport Registration and Integrated Licensing System (TRAILS) and piloting of two subprojects: Ticketable Infringement Notice Automation (TINA) and Management Information Systems Traffic (MIST).
- Approval for development of a Service-wide Corporate Records Management System to enhance efficiency of the corporate records management system by managing administrative records and by providing references, links and accountability to all other corporate records.

1995–96

- The Computerised Offender Identification System fully operational.
- All police stations (more than 300), including those in rural and remote areas, connected to the QPS Computer Network.
- Infrastructure for the new 'client-server' computer environment put in place for a more efficient development and delivery of new applications.
- Work implemented on Polaris.
- The Corporate Electronic Mail project first piloted in Central Region between September and November 1995.
- TRAILS implemented by Queensland Transport in April 1996: 76 police stations online. Initially QPS members were able to make limited driver's licence queries through an interim system using the existing QPS computer system.
- Trials conducted on the Mobile Integrated Network Data Access (MINDA) system to provide police officers on the road with immediate information on vehicles or persons of interest with no need for assistance from the police radio network.
- Operation Phoenix began October 1995 to provide online access through a 'Netscape' computer information service to legislation, operational instructions and other materials of day-to-day importance to all Service members.

1996–97

- E-mail implemented Service-wide from January to July 1996. Usage exceeded one million messages per month this year.
- Implementation of the Bulletin Board statewide ('the number of hits on the Bulletin Board are phenomenal' — Interviewee # 13).
- Phoenix project continuing to be developed. Interactive distance education and training regarding these materials to be provided on Phoenix, also being developed.
- Stage 1 Polaris implemented in October 1996. This stage included:

— The person system — single point of entry to query person information on Polaris and external databases such as TRAILS and NEPI;[23] easy addition of a new person via the warrants system.

— The warrant system — when a name is queried it advises whether that person is wanted on a warrant. Police can then print the warrant from the computer and provide a certified copy. The warrants system can calculate pro-rata payments for persons who have served part of the time of their warrant and OICs are able to assign warrants to staff and view the warrant's progress.

— An address system — TRAILS (Transport Registration and Integrated Licensing System), which replaced the Vehicle and Driver's Licence Systems. Allows address searches to identify who lives at an address and an address history of an individual.

— NEPI — fingerprint system (NAFIS), national stolen vehicle system[24] and National Names Index (missing persons, persons with criminal histories, wanted persons, persons with warnings, persons wanted on a warrant, persons with a domestic violence history and persons with an adverse firearms history). Once a person is located on the system it is necessary to send a message to the appropriate State to obtain further details.

- Polaris Offender History design begun.
- Major modifications to the design of the existing information management system used for weapons licensing to provide for the 1996 Uniform National Gun Control laws, enabling the production of the new Weapons Licence Card. Other developments in relation to the national controls include development and release of computer-based training packages, development of registration procedures, and implementation of a buy-back index for use by police in remote locations.
- CRISP Public Access system implemented, 1 October 1996. This allows for the provision of crime report information to authorised insurance companies (there were 19 insurance companies and 3 loss assessors using the system in 1997) and complainants

23 Polaris has the ability to access the NEPI computer in Sydney to query the Police Reference System. This is a register of persons of interest to police for various reasons. The information on these persons is supplied by all States and could indicate that they are:
- missing persons
- wanted persons
- persons wanted on a warrant
- persons with criminal histories
- persons with adverse firearms histories
- persons with a history of domestic violence.

24 National Vehicles of Interest (NVOI) is a database of vehicle and registration details designed to provide police with direct access to information on stolen, suspect, wanted and recovered vehicles, including driver details. Developed by NEPI this system will be important for operational police — general duties, highway patrols, intelligence, specialist investigations and radio communications, in particular. The first stage allows for national vehicle information and some interstate registration details through the National Exchange of Vehicle and Driver Information System (NEVDIS). Officer safety will be improved as it will include brief notes regarding wanted persons or suspect incidents. Future access to NVOI will be through Polaris. (Wardrop 1999, p. 8)

who can gain access to selected information about their report for a nominal fee. Requests are made through CITEC.

- Improved version of the Incident Management System (IMS).
- Preliminary trials and approval by the Intelligence Management Board for an Intelligence Profiling System that collates information from a number of sources, i.e. CRISP and QUID and presents a profile with a scanned picture image.
- System development for MINDA to provide police with direct mobile access to various databases such as TRAILS, Polaris and marine licensing.
- MINDA operational from April 1996.
- Development of a policy framework, policies and procedures for the security of information. Its objectives were to ensure confidentiality, integrity, privacy and availability of all information assets, services and systems that support the Service's functions, and to ensure that they are maintained in accordance with the strictest Australian standards.
- Use of QUID extended to all District and Station Intelligence Officers, Southern Region.
- Computer-based training for Polaris, CRISP and Juvenile Justice completed and distributed statewide.
- Marine Search and Rescue Management implemented March 1997.
- Database of job logs of police activities in schools implemented February 1997.
- 386 Apple Macs delivered and installed.
- The five existing computer networks were consolidated into a single corporate network.
- Corporate Data Server installed.
- Service Level Agreements completed with Queensland Transport and e-mail. Service Level Agreements under development for Polaris Releases I and II, Weapons, IMS, Department of Justice, Camera Detected Offences System, Polaris training. Planned agreement with NEPI.
- Data warehousing project implemented by the Information Resource Centre to provide crime-related information.
- In 1996 the Service received a gold medal at the National Technology Awards for its CRISP computer system.
- December 1997 — introduction of a community policing initiative in a Brisbane suburb (Springfield), whereby every house was provided with a computer and access to the Internet, and was linked to the local police officer who was centrally located within a house in the suburb. Every house is kept informed of local policing issues and problems.

1997–98

- February 1997, re-scoping of the Corporate Records Management System. Project team mobilised January 1998.
- Release of the Virtual Library statewide on the Bulletin Board — December 1997.
- QPS Internet site released mid-1997.
- Electronic Warrants released.
- Controlled data entry (Crime Reports) introduced in large police stations by station staff.
- Help Desk available 24 hours.
- Speed of processing interstate criminal histories improved.
- Introduction of night shifts for data entry personnel to enable criminal histories to be updated more quickly.
- Creation of Polaris Section and appointment of Polaris Director.
- Release of Query Address feature on Polaris in August 1998. This feature lists all names recorded on Polaris and/or TRAILS that are associated with a specific address, both past and present.
- Partial Network upgrade to frame relay.
- Secure Gateway provided.
- CITEC contracted to redesign the Property Crime Squad's Stolen Property Investigations and Recovery System (SPIRS) for statewide use. SPIRS is a computer system designed to increase the identification and recovery of stolen property — the system collects and stores data from pawnbrokers and second-hand dealers. The data can be queried to show the interaction of people, property and a pawnbroker or second-hand dealer (referred to as a licensee).
- Evaluation of MINDA through to 1998–99.
- Introduction of Maverick.
- Radio communication and infrastructure upgraded.
- Due to requirements of the new *Police Powers and Responsibilities Act 1997*, the Custody/Search Index was implemented to record details of all persons who are arrested, detained for questioning, investigated or searched, or otherwise held in custody.
- The CRISP electronic supplementary forms and the Police Use of Force Incident Reports (such as the use of Oleoresin Capsicum Spray) were introduced. These were designed to enhance the CRISP recording of supplementary information and incident reports and were provided as an alternative to telephoning or faxing information to the Crime Management Section. Once submitted, these forms are transferred electronically to the Crime Management Section.

- Since January 1998, all Australian States provide data to the Violent Crime Linkage Analysis System (ViCLAS), which is a national database designed to link and analyse predatory crimes of violence such as murder and sexual assaults. In Queensland, the Violent Crime Analysis Unit (ViCAU) is located within the Bureau of Criminal Intelligence Queensland (BCIQ). The officer in charge of ViCAU is the State Coordinator for ViCLAS. ViCAU is responsible for collection, collation, analysis and dissemination of information relating to offences of this nature. ViCLAS overseeing officers are regional crime coordinators, Detective Superintendent, State Crime Operations Command and the Crime Manager of the CJC.

1999–2000

- $10.8 million allocated to a range of information technology programs 1999–2000.
- Polaris version 1.8 released May 2000. Includes address update, inquiry log, added TRAILS functionality, charges database, warrants update and reported linking.[25]
- CAD implemented in South East Region and Ipswich District.
- Year 2000 compliance activities.
- The Queensland Intelligence Database (QUID) was converted to the Australian Criminal Intelligence Database (ACID).
- SPIRS access became available to selected intelligence and Criminal Intelligence Bureau (CIB) staff.
- 200 MINDA units available — service to the units, previously undertaken by Queensland Transport, will be undertaken by the QPS from 2001, but lack of funding may be a problem (Interviewee #10, second interview).
- Crim Trac introduced. The Federal Government spent $50 million on this state-of-the-art national crime investigation system, which is a collaborative effort between national police organisations, Queensland Health, Corrective Services, Justice Department etc. Components of Crim Trac will be phased in and subject to jurisdictional and financial logistics. Initial phases of Crim Trac will include:
  - — the National Automated Fingerprint Identification System (NAFIS), which uses livescan technology
  - — a DNA database.
  - — linking of existing jurisdictional information resources such as domestic violence and weapons indexes, criminal records, stolen vehicles and persons of interest, including missing persons
  - — a national sex offender register.

25 This version was expected to be released late 1998.

- Several stand-alone databases and forms packages were developed for limited access:
  - the high-speed pursuits database (State Traffic Support Branch).
  - the automated forms system for the Prostitution Legislation Authority (the *Prostitution Act 1999*).[26]
- Upgrading took place of the Service's mainframe and the desktop computer network.
- The final phase of the Secure Gateway project was completed allowing the Service to provide a significant number of members with access to the Internet and external e-mail (as of November 2000, there were 1500 licences — Interviewee #10 second interview).
- All work-stations were connected to the Queensland Government Network.

Future developments

- It is anticipated that Polaris 1.9 (release date to be announced) will include:
  - — photo ID cards and the Photo Name Board, dependent on appropriate access agreements with the Queensland Corrective Services Commission or other corrective services agencies
  - — information relevant to the new legislation on drug diversion (*Police Powers and Responsibilities Act 2000*).
- Polaris II (release date as yet unplanned) will include the integration of a lot of current systems including single entry of basic information at the beginning of the charging process:
  - — The information obtained on CRISP will be used by Polaris to begin the charging process. It will no longer be a requirement of an arresting officer to contact CRISP by telephone to receive a crime number in the event of an arrest where the offence has not previously been reported. The information will be entered on the system by the arresting officer and will be updated by the QP9[27] when it is electronically transferred to the CRISP data-entry operators.
  - — Bench Charge Sheets
  - — Summary of defendant's charges
  - — Charge book insert
  - — Summons, QP13 (fingerprint form)
  - — Notice to Allege Previous Convictions

26 This database has been transferred to the Prostitution Licensing Authority, but is not used due to limitations in data capture, flexibility and analysis.

27 A court brief or QP9 is the document provided by the arresting officer to the police prosecutor that details the police officer's recollection of events which led to the arrest.

— Notice to Licensee (24-hour suspension)

— QP9 (court brief).[28] This will be completed in conjunction with the Courts Modernisation Process. Once all courthouses have the ability to transfer information electronically (stage 2), the courts will be able to update Polaris information on offender histories in a more timely fashion.

— Vehicles and Vessels searches will replace 'Query Vehicles' in the current QPS system. This will be designed to coincide with Queensland Transport's TRAILS system development. The first stage of Vehicles and Vessels will build appropriate interfaces so that all relevant QPS information systems can gain access to the new TRAILS registrations system. TRAILS information will display a Vehicle Identification Number (VIN) that can be used to access a complete history of that vehicle and its owners.

- Polaris III will include arrest and custody (Custody Index), the Search Register (Police Powers and Responsibilities Act), seized property, tapes management (Tapes Index) and exhibits (found property/exhibits and drugs exhibits).
- To align itself with the Queensland Government strategy, the QPS has instigated the Desktop Replacement Project, which will:

  — replace all Apple® class machines with computers running the Windows 2000® operating system (there will be a transition period of several years whereby both systems will be running)

  The target date for delivery of the first PCs was April 2001. It is expected that the changeover will occur by July 2002 (QPS Bulletin Board, Desktop Replacement Home Page, 2000).

  — establish an 'Active Directory Infrastructure' (i.e. one log-in to file servers for e-mail, external mail, internet and desktop access)

  — increase the computer-to-person ratio — the project budget identifies the need to increase the number of PCs by 1000 extra machines in years 2 and 3 and a further 500 in year 4 [29]

  — provide a standard common version of the Microsoft Office Suite (i.e. Word, Excel and PowerPoint)

  — establish a central forms service

  — provide software and hardware audit, and asset capability

  — implement a corporate change-control mechanism to apply to all desktop computers.

---

28 All QP9s will be accessible to police online as well as to Prosecutions and other external agencies such as the Office of the Director of the Department of Public Prosecutions and the Department of Corrective Services.

29 There are currently 6500 PCs throughout the State — the project will install about 7500 PCs overall (Interviewee #10, second interview). The new computers will not have a floppy drive. This will (a) restrict access to software programs that have not been approved corporately and (b) centralise the installation of all corporate systems statewide.

- Future mobile data releases hope to include:
  - computer-aided dispatch
  - field access to, and update of information from, existing systems and applications
  - mapping of Automatic Vehicle Location (AVL) and Officer Down notification capability
  - automatic update of the QPS Activity Report Index (ARI) in relation to the interception of persons and vehicles
  - ability to generate patrol logs
  - direct capture of property seizures, NTAs, Search Register and detaining information as required under police powers legislation
  - record and print statements at the scene
  - e-mail and Bulletin Board availability.
- The Service will move toward information-based traffic operations, expansion of the traffic camera system, the wider use of information derived from incident management systems and the full implementation of a Traffic Complaints System to provide information on areas of community concern.
- In the longer term, a CAD system will be considered for each region with a view to achieving consistency in dispatch systems across the State.
- Further developments to Crim Trac will occur.
- The library will be completely electronically web-based.
- The Crime Reporting Information Management System (CRIMS) is a data warehouse that downloads CRISP and other relevant data (such as CAD and traffic information) on a daily basis. This system is currently accessed by statisticians within the Information Resource Centre (IRC), and some intel officers and statisticians use the data for decision support, problem-oriented policing and customer and client servicing (see the 1996 timeline). There are plans for this interactive system to be implemented statewide for police and management to be able to interrogate the data themselves, but funding and policy change are required for it to progress (Interviewee #2). By mid-1998 an estimated half a million dollars had been spent on developing a prototype.
- Some of the interviewees identified a need for an IT-based case-management system for major incidents such as a prison break, an extortion attempt or a major drug operation (such as Promis, which is currently operated by the Australian Federal Police).

References

Abt Associates 2000, *Police Department Information Systems Technology Enhancement Project (ISTEP)*, Department of Justice, Office of Community Oriented Policing Services, Washington, DC.

Ackroyd, S., Harper, R., Hughes, J.A., Shapiro, D. & Soothill K. 1992, *New Technology and Practical Police Work*, Open University Press, Buckingham.

Barley, S. 1986, 'Technology As an Occasion for Structuring: Evidence From Observations of CT Scanners and the Social Order of Radiology Departments', *Administrative Science Quarterly,* 31, 1986, pp. 78–108.

Bingham, M. 1996, *Report on the Review of the Queensland Police Service*, Prepared for the Honourable Russell Cooper, Minister for Police and Corrective Services and Minister for Racing, Brisbane.

Chaiken, J., Crabill, T., Holliday, L., Jaquett, D., Lawless, M. & Quade, E. 1975, *Criminal Justice Models: An Overview*, Santa Monica, California: RAND [Cited in Manning (1992a)].

Chan, J. 1999, 'Governing Police Practice: Limits of the New Accountability', *British Journal of Sociology*, 50(2), pp. 249–68.

—— 1997, *Changing Police Culture: Policing in a Multicultural Society*, Cambridge University Press, Melbourne.

Colton, K. (ed.) 1978, *Police Computer Technology*, Lexington, Mass. Heath, D.C. [cited in Manning, 1992a].

Criminal Justice Commission 2001a, *Integrity in the Queensland Police Service: QPS Reform Update*, vol. 1.

—— forthcoming, Integrity in the Queensland Police Service: QPS Reform Update, vol. 2.

—— 2001b, *Criminal Justice System Monitor*, vol. 5.

—— 2000a, *Police Strip Searches in Queensland: An Inquiry into the Law and Practice*.

—— 2000b, *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*.

—— 2000c, *Prisoner Numbers in Queensland: An Examination of Population Trends in Queensland's Correctional Institutions*.

—— 1999, *Police Powers in Queensland: Notices to Appear*, Research Paper Series, vol. 5, no. 2.

—— 1998a, *Beenleigh Calls for Service Project: Evaluation Report*.

—— 1998b, *Policing and the Community in Brisbane*.

—— 1997a, *Police and Drugs: A Report of an Investigation of Cases Involving Queensland Police Officers*.

—— 1997b, *The Cost of First Response Policing*, Research Paper series, vol. 4, no. 2.

—— 1997c, *Gold Coast District Negotiated Response Trial: Survey Findings*.

—— 1994, *Implementation of Reform within the Queensland Police Service: The Response of the Queensland Police Service to the Fitzgerald Inquiry Recommendations*, CJC, Brisbane.

Davids, C. & Hancock, L. 1998, 'Policing, Accountability, and Citizenship in the Market State', *Australian and New Zealand Journal of Criminology*, 31(1), pp. 38–68.

Dean, M. 1999, *Governmentality: Power and Rule in Modern Society*, Sage, London.

Department of Communication and Information, Local Government and Planning, Queensland, 1999a, Information Standard 24: *Information Management, Policies for the Management of Information within Government*. Retrieved 20 April 2000 from http://www.dcilgp.qld.gov.au/comminfo/download/is24.pdf>.

—— 1999b, Information Standard 16: Management, Agency Information Steering Committees. Retrieved 20 April 2000 from http://www.dcilgp.qld.gov.au/comminfo/download/is16.pdf>.

Earl M.J. 1989, *Management Strategies for Information Technology*, Prentice Hall, UK.

Ericson, R. V. & Haggerty K. D. 1997, *Policing the Risk Society*, University of Toronto Press, Toronto.

Fitzgerald, G.E., 1989, *Queensland Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct*, Government Printer, Brisbane.

Giddens, A. 1984, *The Constitution of Society*, Polity Press, Cambridge.

Grace, R. undated, *Computer Technology and Criminal Investigation: Two Decades of Progress*. Vedette, no. 164.

Harper, R.R. 1991, 'The Computer Game: Detectives, Suspects, and Technology,' *British Journal of Criminology,* 31(3), pp. 292–307.

Henman, P. 1996, Constructing Families and Disciplining Bodies: A Socio-technical Study of Computers, Policy and Governance in Australia's Department of Social Security, PhD thesis, University of Queensland.

Hough, J.M. 1980a, *Uniformed Police Work and Management Technology*, UK Home Office, London.

——1980b, 'Managing with Less Technology — The Impact of Information Technology on Police Management', *British Journal of Criminology*, 20(4), pp. 344–57.

Howell, J.M. & Higgins, C.A. 1990, 'Champions of Technological Innovations', *Administrative Science Quarterly*, 35, pp. 317–41.

Legosz, M. & Brereton, D. 2001, *On the Road with Maverick: A Case Study of the Impact of Information Technology on Policing*, paper presented to the 15th annual conference of the Australian and New Zealand Society of Criminology, Criminology in the 21st Century: Public good or private interest? Melbourne, February 2001.

Leishman, F., Loveday, B. & Savage, S.P. (eds) 1996, *Core Issues in Policing*, Longman, London.

Machin, T. 1997, *Evaluation of Polaris Level 3 Training*, University of Southern Queensland, Toowoomba.

Manning, P. K. 1996, 'Information Technology in the Police Context: The "Sailor" Phone', *Information Systems Research*, 7(1), pp. 52–62.

—— 1992a, 'Information Technologies and the Police', in Tonry, M. & Morris, N. (eds) *Modern Policing: Crime and Justice*: A Review of Research, vol. 15, pp. 349–98, University of Chicago Press, Chicago.

—— 1992b, 'Technological Dramas and the Police: Statement and Counterstatement in Organizational Analysis', *Criminology*, 30(3), pp. 327–46.

Miller, P. & Rose, N. 1990, 'Governing Economic Life', *Economy and Society*, 19(1), pp. 1–32.

Mortimer, B. 1998, Conceptualisation of Policing Information and its Relationship with Problem Oriented Policing, Thesis submitted in partial fulfilment of the requirements of the degree of Master of Social Planning and Development. Department of Anthropology and Sociology, University of Queensland.

Mullen, K.L. 1996, The Computerization of Law Enforcement: A Diffusion of Innovation Study, PhD thesis, University of Albany, State University of New York.

O'Malley, P. & Palmer, D. 1996, 'Post-Keynesian Policing', *Economy and Society*, 25(2), pp. 137–55.

Orlandi, M., Landers, C., Weston, R. & Haley, N. 1997, 'Diffusion of Health Promotion Innovations' in Glanz, K., Lewis, F.M. & Rimer, B.K. (eds), *Health Behaviour and Health Education: Theory Research and Practice*, Jossey-Bass, San Francisco.

Orlikowski, W.J. 1996, 'Improvising Organizational Transformation Over Time — a Situated Change Perspective', *Information Systems Research,* 7(1), pp. 63–92.

Orlikowski, W.J. & Gash, D.C. 1994, 'Technological Frames — Making Sense of Information Technology in Organizations', *ACM Transactions on Information Systems*, 12(2), 174–207.

Orlikowski, W. & Robey, D. 1991, 'Information Technology and the Structuring of Organizations', *Information Systems Research,* 2, pp. 143–69.

Power, M. 1997, *The Audit Society: Rituals of Verification*, Oxford University Press, Oxford.

Public Sector Management Commission, *1993 Review of the Queensland Police Service*, Goprint, Brisbane.

Queensland Police Service 2000, *Information Management Operational Plan*, QPS Bulletin Board.

—— 2000a, *Queensland Police Service Annual Report, 1999–2000.*

—— 2000b, *Environmental Scan,* Office of the Commissioner Policy Unit. QPS Bulletin Board.

—— 1998a, *Statistical Review 1997–1998*, QPS, Brisbane.

—— 1998b, *IMD Client Survey and Service Quality Report 1998,* QPS, Brisbane.

—— 1997, *IMD Client Survey and Service Quality Report 1997,* QPS, Brisbane.

—— 1995, *Information Strategic and Infrastructure Plan 1995–2000*. QPS, Brisbane.

—— undated (a), *Information Management Strategic Plan for 1999–2001*, QPS Bulletin Board, accessed 8 September 2000.

—— undated (b), *A Guide to Problem-Oriented and Partnership Policing*, Brisbane.

—— 1991–92 to 1999–2000, *Statistical Reviews* (annual), Brisbane.

Queensland Police Service Review 1996, *Report on the Review of the Queensland Police Service* [Bingham Review], Prepared for the Honourable Russell Cooper MLA, Minister for Police and Corrective Services and Minister for Racing, QPS Review Committee, Kingswood Press, Brisbane.

Report on a Commission of Inquiry Pursuant to Orders in Council [Fitzgerald Report], 1989 Government Printer, Brisbane. Title of Inquiry: Commission of Inquiry: Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct [Fitzgerald Inquiry] 1989, Chaired by G. E. Fitzgerald, QC.

Reuiss, E. & Ianni, F. 1983, 'Street Cops and Management Cops: The Two Cultures of Policing' in Punch, M. (ed.) *Control in Police Organization*, MIT Press, Cambridge.

Rheinier, B., Greeless, M.R., Gibbens, M.H. & Marshall, S.P. 1979, *Crime Analysis in Support of Patrol*, Law Enforcement Assistance Administration report, US Government Printing Office, Washington, DC [Cited in Manning, 1992a].

Robey, D. & Sahay, S. 1996, 'Transforming Work Through Information Technology: A Comparative Case Study of Geographic Information Systems in County Government.' *Information Systems Research,* 7(1), pp. 93–110.

Rogers, E.M. 1995, *Diffusion of Innovations* (4th Edition), Free Press, New York.

Sabatier, P. 1986, 'Top–down and bottom–up approaches to implementation research: a critical analysis and a suggested synthesis', *Journal of Public Policy*, 6, pp. 2-48.

Sackmann, S. 1991, *Cultural Knowledge in Organizations*, Sage, Newbury Park, CA.

Schein, E. 1985, *Organizational Culture and Leadership*, Jossey-Bass, San Francisco.

Sparrow, M. 1991, 'Information Systems: a Help or Hindrance in the Evolution of Policing?', *The Police Chief,* 58 (4, April), pp. 26–44.

Van de Ven, A.H. & Rogers, E.M. 1988, 'Innovations and Organizations: Critical Perspectives', *Communication Research,* 15(5), pp. 632–651.

Wardrop C. 1999, 'NVOI is … ', *Police Bulletin*, no. 174, QPS, Brisbane.

Yates, J. & Van Maanen, J. 1996, Editorial Notes for the Special Issue, *Information Systems Research,* 7(1), pp. 1–4.

Note: A paper by J. Chan, 'The Technological Game: How Information Technology Is Transforming Police Practice', published in *Criminal Justice* in 2001, volume 1, issue 2, draws on the results and discussion from several sections of this report.