OPENING ADDRESS

Michael Tate
Senator
Federal Minister for Justice
Canberra

IN 1990, THE PRIME MINISTER, BOB HAWKE, ISSUED A CHALLENGE TO ALL Australians. He said:

> No longer content to be just the lucky country, Australia must become the clever country (Hawke 1990).

That challenge is one, I am pleased to say, that has been taken up by the policing profession in Australia. Indeed, for some years now, policing, with the strong support of all Australian police ministers, has become cleverer. We have seen the establishment of the National Police Research Unit (NPRU), the Australian Bureau of Criminal Intelligence (ABCI), the National Exchange of Police Information (NEPI), the Cash Transactions Reports Agency, the National Institute of Forensic Science and the emergence of the Australian Institute of Criminology as an important agent in policing research.

Overlaying all this has been the dramatic recognition by Australian police forces that they need to be smarter than the criminals. That has meant a commitment to technology at a far greater level, rather than the old method of throwing more manpower into the field.

This 'technology first' approach is absolutely vital to the fight against crime and conferences such as this enable policing in Australia to keep abreast of contemporary technological advances.

I hardly need to remind delegates to this conference that, while ever we live in a climate of little real growth in budgetary allocations, all agencies represented here must critically examine every opportunity to improve their performance through the use of technology.

Trends and Future Directions

With respect to trends and future directions in police technology there is no doubt that major advances have been, are being, and will continue to be, made in the use of information technology. The emergence of nationally-

based and accessed databases has resulted in incalculable benefits to law enforcement generally, and policing in particular. I am greatly impressed by the national automated fingerprint system which I believe is demonstrably superior to systems in place anywhere else in the world. The Australian Passenger Automated Selection System is equally impressive, so much so that Australia has exported its technology and expertise to the South East Asian Region, specifically Thailand and the Philippines.

Discussions with my policing counterparts around the world confirm my view that, in the Cash Transactions Reports Agency, Australia has one of the most advanced computer-based systems in the world for following the money trail and providing the structure to fight that most insidious of modern criminal activities—money laundering.

The Australian Government has committed funds to the establishment of the Law Enforcement Access Network (LEAN) on a permanent basis. This follows a highly successful pilot of the network in which many of your agencies participated.

As to forensic science—an area subject to much justified criticism in recent years—I, and my colleagues on the Australian Police Ministers' Council, am confident that the National Institute of Forensic Science, under the guidance of Mr Justice Phillips, will win back the confidence of the Australian community for this vital area of our criminal justice system.

I mentioned earlier the national common police services, such as the National Exchange of Police Information (NEPI), the National Police Research Unit (NPRU) and the Australian Bureau of Criminal Intelligence (ABCI):

- the National Exchange of Police Information (NEPI) is responsible for the national fingerprint system discussed above and for the establishment and maintenance of national computer systems;

- the National Police Research Unit (NPRU), through its equipment advisory forum program, is progressively examining areas of equipment and technology where common standards may be adopted and common difficulties overcome; and

- the Australian Bureau of Criminal Intelligence (ABCI) has established a national intelligence database in the drug enforcement area.

These bodies, oversighted and managed by all Australian jurisdictions, ensure that policing is ably served in the application of technology.

Delegates to this conference would be aware that, as Minister responsible for the Australian Federal Police at the national level, I have no direct involvement in community policing issues such as traffic policing. Nevertheless, I acknowledge that these are 'real issues of the day' for many delegates and for all my colleagues on the Australian Police Ministers' Council. I congratulate those involved in the research on these important community policing technologies and commend the relevant sessions of this conference to delegates.

I wish to add at this point that governments have a role to play in this area and, I am pleased to say, have indeed played that role. Technological advances must be underpinned and supported by a legislative framework. At the Federal level, there are legislation that do that job. Recent amendments to the *Crimes Act 1914* underpin the investigation of computer crime, the *Cash Transaction Reports Amendment Act 1991*

supports the agency in its vital work, and the *Telecommunications (Interception) Act 1979* enables relevant agencies to gather evidence of criminal activity. The *Proceeds of Crime Act 1987* assists markedly in the fight against organised crime and money laundering, and the *Crimes (Investigation of Commonwealth Offences) Amendment Act 1991* requires, inter alia, the mandatory recording of interviews which will greatly enhance the prosecution of Commonwealth offences.

Conclusion

As is evident from the conference program, Australian law enforcement agencies have made a considerable investment in the application of technology that will assist them in their work. This investment is proving, and will continue to prove, that Australia is indeed becoming smarter and cleverer. To succeed in combating crime, police and law enforcement agencies must be smarter than the criminals. I believe that this conference will prove that they are.

I congratulate the Australian Institute of Criminology and the National Police Research Unit for putting this conference together and wish all delegates well in their deliberations.

I have great pleasure in formally declaring open the 1991 Asia Pacific Police Technology Conference.

Reference

Hawke, R.J. 1990, speech presented at the Australian Labor Party Election Policy Launch.

LAW ENFORCEMENT AND TECHNOLOGY

Robert Hamdorf
Chief Superintendent
Deputy Director
National Police Research Unit
Adelaide
South Australia

IN AN ENVIRONMENT IN WHICH CRIMINALS HAVE HUGE FINANCIAL backing to concentrate on often narrow fields of endeavour, law enforcement agencies around the world have increasingly become reliant upon sophisticated technology to aid them in the fight against crime. Invariably, behind the financial backing is a proficient management structure. It is no wonder that the police become so frustrated in their efforts to keep up, let alone get in front.

Although Australian policing is becoming more sophisticated through its use of technology, it remains behind many other developed nations. However, world crime is encroaching on Australia at an ever-increasing rate with home-bred crime taking up the modus operandi gleaned from overseas.

Within that framework, if I were to ask for law enforcement agency's understanding of the term 'technology', the most common response would likely be: 'it is that which is needed to keep pace with the modern day criminal but which law enforcement agencies cannot get enough of'. Also, if each area within a law enforcement agency were asked the same question, each would have its own demand for better technological means to enable better job performance.

Over the next three days, delegates to this conference will be able to participate in enlightening presentations from people recognised as being at the forefront in their field. Insights into the acquisition of technology, as well as the difficulties in identifying the most appropriate technology and the juggling of priorities, will be given. There is little value in purchasing equipment and software if it is about to be superseded, is too narrow in application, cannot be expanded, or is incompatible with that used by counterparts in other places. There is, therefore, a need to have a broader, national perspective in this process.

Traffic policing, of course, has been moving inexorably away from reliance upon the policeman behind the wheel of the car or motorcycle following and timing an

offender for three-tenths of a kilometre between streets 'X' and 'Y'. Technology has not only made it easier to prove the offence but has enlarged the capture net. Many argue that the adoption of science in the traffic arena is nothing more than a revenue raising effort, however, people fail to understand the real aim: that is, to make the roads a safer place to drive. There seems to be an 'Australian' view that, although a person might be speeding, drink driving, and so on, it is 'unfair' to use radar, speed cameras, breathalysers and similar technology. Road deaths and serious injuries have diminished. Notwithstanding the advances, one must also be vigilant of likely health threats arising from the types of technology being utilised, for example, the microwave radiation associated with speed radar.

Crime investigations have traditionally been an area where science has been applied in ever-increasing and more sophisticated ways. From the examination of fingerprints, to the electron microscope and beyond, the realm is ripe for advances which will heighten the probability of offender recognition and successful prosecutions.

Statistics is an area in which law enforcement agencies must develop more exacting and useful information. Comparability of information is always difficult on a national scale, but at the local level there is increasing reliance on statistical data to highlight problem crimes and appropriate geographical areas for targeting to enable more effective application of effort. The large data banks of crime-related information married with 'number crunching' computers are essential tools in providing strategies and tactical information to operational police.

Communications systems are lifelines of every police member. The reliability of systems and their flexibility for multiple applications, such as data transmissions, are opening the way to mobile computer terminals and the ability for the patrol officer to enter crime report, accident, offender or witness details directly onto the mainframe computer by way of audio coupling or floppy disc transfer. Is it possible that the frontline of policing could become paper free?

Vehicles are a major capital expenditure item for any police organisation. Due to the nature of police work, there is the potential for vehicles to play a large part in secondary major expenditures through the loss of human life, injury to staff and resultant absenteeism, mechanical repairs and vehicle replacement due to legitimate use and misuse and poor maintenance. Because vehicles are used so diversely and spread so widely throughout each state and territory, it has become more difficult to ensure that vehicles used are the most appropriate for their application and are maintained to a degree that will minimise danger to the police and public alike. Fleet management is a very important part of running a law enforcement agency.

Computer technology has become essential. Computers come in all shapes and sizes and each section or unit will have a favourite make, model and software which most suits their application. The task of management is not only to ensure that the computer supplied will do the job required, but also that it is compatible with other units and systems within the organisation. This is not an easy task and, regardless of how sound a decision might be, there may still be dissenting views.

Prior to and since my time with the National Police Research Unit I have read much about the need for innovative technology and the uses to which it can be put. Given money and time, imagination is generally the only limiting factor. However, when glancing through a newspaper, I saw an advertisement, obviously by a computer company, which provided as part of its message a rather sobering thought which is relevant to the theme of this conference. The advertisement read in part:

> If you believe technology alone will improve productivity . . . without doubt, advances in technology have led to faster, more powerful computers. The trouble is that while these computers have automated the office they haven't significantly improved productivity ('Wang' advertisement, *The Australian*, 22 October 1991, p. 7).

There is, within the law enforcement industry, a need for effort to be made to keep pace with trends in crime. The type of crime and the modus operandi used demands that police continually search out better and more effective ways of combating the crime problem. Similarly, there is little point in conducting research and finding answers if the results are not acted upon. Although set in a private enterprise framework, comments by Professor David Midgley of the Australian Graduate School of Management seem relevant. He wrote, about public expenditure and commercial outcomes of Public Sector Research and Development:

> It may be that we have an excess of public sector 'R' and relatively little 'D' making it difficult for companies to utilise the results of public research (*The Australian Magazine*, 8 October 1991, p. 4).

Professor Midgley went on to discuss the need to develop technology to suit the market requirements. Does this not sound a lot like developing technology to suit emerging crime trends?

Another quote which links with the thoughts of Professor Midgley is that by Peter McGauran, the Opposition spokesman for Science and Technology. Among other things he concluded a thought with 'mere survival means change, adaptability and technological innovation' (McGauran 1991, p. 218). Adaptability and innovation are important terms for today's police managers.

As the computer is the central power of much of current and future technology to be utilised by law enforcement agencies, it is interesting to see that the Japanese computer community is developing the Fifth Generation Computer which is intended to have artificial intelligence and thus the ability to think for itself. Innovation of the first order, it opens new worlds for policing both as an aid and a tool to commit and hide criminal activities. How will we as a police community respond to this type of development?

A final thought relates to the importance of *ethics* within the context of the technological environment. To a large extent the use of the many aspects of technology in support of the policing role has provided indisputable corroboration of police evidence, thus reducing the attack upon integrity. However, the same technology demands that the ethical questions associated with its application, and the subsequent use of material or evidence thus gained, is within the law and the spirit of the intention of the law. Abuses could, in time, deny its use to police. Law enforcement agencies must therefore take pains to be scrupulously careful with our use of these tools of trade.

References

McGauran, P. 1991, 'Editorial', *Search*, vol. 22, no. 7, October/November, p. 218.

Midgley, D.F. 1991, 'Giving the Customer What They Want', *The Australian Magazine – special magazine 'Focus on International Week'*, 8 October, p. 4.

MANAGING THE ACQUISITION OF TECHNOLOGY

Bruce Window
Director
Technical Services
Queensland Police Service

FOR THIS PAPER, THE DEFINITION OF *TECHNOLOGY FOR POLICING* WILL BE:

> Knowledge and equipment that deals with science and engineering and its practice as applied to policing.

Technology can cover a diverse range of policing and support activities—equipment from radar guns, to accounting spreadsheets, to radio systems and even to forensic science. In fact, the range of knowledge and equipment is almost limitless. Potential costs for projects under this umbrella covers a similar breadth.

The study of management of the acquisition and utilisation of technology is a very broad field and at least one Australian university has a masters degree in this specific subject area. This paper, while touching the subject briefly, can only hope to introduce the reader to the possibility of some new concepts or provide a reminder of some old.

There are at least three key issues which require addressing and resolution for any organisation wishing to manage its technological acquisitions. They are:

- Why do we want to acquire the technology?
- How should we go about the acquisition?
- What, if anything, needs to be done after the technology is in place?

While there are other issues involved in this particular management exercise, it is suggested that these three are essential for a successful acquisition program.

Reasons for Acquisition

The most obvious reasons, or those most often quoted, for the acquisition of technology include better efficiency or effectiveness. Many books, papers and internal reports address these issues in detail. They are often used as primary reason or justification for vast expenditure on resources of both time and money. Without degrading the importance of these, there are other, often unstated, factors driving the desire for acquisition. These factors should not be surreptitiously swept under the carpet or kept out of discussion. Rather they should be honestly recognised and used in any measurement of the success of the technology implementation.

The reason 'to keep up with the technology used by offenders against society' is often used as an argument or defence when justifying purchases, but how often is the desire to keep up with another agency an unstated reason? Alternatively, the improvement of morale or the desire to make officers feel 'better, needed, or wanted' is sometimes just as important, although not stated, as the efficiency and effectiveness above. There may even be political motivation behind the introduction of new technologies. All of these additional valid reasons or issues need addressing in any program for technological acquisition.

The textbooks emphasise the importance of evaluation for any management program but, if all the reasons for acquisition are not being acknowledged, the evaluation is either incomplete or irrelevant. The reasons for the acquisition of new technology need to be fully understood, not just known. The responsible manager's understanding of all these reasons will greatly assist in the analysis and assessment of any program prior to approval being given. If addressed in an open and realistic manner with the various factors taken into account, better implementation will result or perhaps, if inappropriate, not even go ahead.

How to Introduce Technology

The beginning of the introduction of any new technology spawns a plethora of processes and activities—budgets, schedules, specifications, tenders, reports, unions, training and more. The mechanics of many of these are well covered in other literature, therefore this paper will comment on aspects of only four.

Specifications

Specifications have traditionally been written as technical documents with the purchaser having done a large amount of work to describe in purely technical terms what is required from the proposed acquisition. Sometimes the specification document is written to exclude some, or even all but one, of the potential suppliers from tendering. Specifications of this form assume the purchaser knows the marketplace, or perhaps does not want to acknowledge an alternate supplier of solutions, rather than predetermined equipment.

An alternate form of specification is the functional specification. With this document the problem is defined and a solution sought. It does not mean that there are no technical requirements. There will always be a necessity for these, for example, 240v power input, Australian Government Open Systems Interconnective Profile (GOSIP) compliance for computer purchases, colour temperature of lights, and so on. What it does mean is that the technical requirements are of a clarifying nature to the functional requirements. This process can mean additional effort, initially in defining

exactly what is needed from the equipment (however, this should have been an output from understanding the reasons for acquisition), and subsequent evaluation of quotations or tenders. It may even be useful to provide some type of briefing for suppliers prior to their responses being prepared.

With the extra work involved there has to be some benefit to any organisation embarking on this path. It comes from a far better understanding achieved through the process of the problems to be solved by the technology and a sharper focus on the implementation needs.

Acceptance of change

Acceptance of change is the stumbling block for many technology projects. Without the end user accepting the change as positive and worthwhile, there is little hope of a successful outcome. It is essential for the ownership of any technological change to rest with those who are affected by it. If workers see advantage in change they will make it work, if not they hinder its adoption. To have input into the decision-making processes and to be involved in planning engenders support rather than obstruction.

Consultation

The decision to consult, or otherwise, with the unions is often synonymous with their decision to support or oppose. Make the decision wisely because the emotion evoked can obscure subsequent clear thinking on both sides.

Training

For large projects, training needs to be analysed, designed, trialed and then re-analysed with continuing changes if required. Smaller projects may not need such extensive work, but without training all are doomed to failure. This does not mean that all training must be carried out by expensive providers at distant resorts. It does mean that appropriate training is provided for all staff and, if an organisation is to become technologically rich, training must continue to be provided and be an integral part of any operational budget, not just the initial acquisition budget.

Evaluation

The process of evaluation should have started its design phase when the reasons to acquire new technology were first identified. Certainly a clear understanding of the reasons will provide obvious pointers to the criteria for evaluation. Organisations should not dismiss or move away from assessing whether all the reasons for acquisition have been satisfied during the actual process of implementation and utilisation. If no cognisance is taken of those strong but perhaps less altruistic reasons and their satisfaction, then they will surely surface again and again until their eventual resolution.

It is not uncommon for evaluation to be addressed after an introduction or implementation is completed. This approach prevents 'before and after' comparisons and removes the possibility of important feedback to both managers and staff, as well as other stakeholders with an interest in the issue.

Any large scale implementation project, or any technology introduction that significantly impacts on staff procedures and practices, must have progressive evaluation

and a range of built-in tools to assist in the process. These can range from the obvious and almost trivial (but none the less important)—for example, minuted staff meetings—to systems that take as much as 30 or 40 per cent of the total implementation budget—such as the introduction of computerisation and a totally new way of processing information. While an expenditure of that level may seem high, without it such a project could easily incur greater cost overruns or even be totally aborted.

Many texts have been written on this subject and project managers should be conversant with them.

Supplier and external stakeholder feedback is a frequently neglected area. A common government procedure in Australia of deciding major tenders and providing little or no formal feedback to organisations who expended significant time and effort to submit a tender is counter productive in the longer term. It appears to be much easier to send a 'thanks, but no thanks' letter of less than six lines than to have public debriefing sessions and private explanations of each organisation's strengths and weaknesses with respect to the intending purchasers selection criteria. A recent tender in Queensland, where this process was followed, had over 30 per cent of respondents subsequently communicate their very positive appreciation of the opportunity. Longer term advantages are that the quality of responses will improve with time and that suppliers will know better the expectations placed on them.

What if the predictions are wrong? This particular fear is paramount in some managers' minds when the thought of evaluation is introduced, particularly if that evaluation has quantitative measurements. There seems to be a concern that if numeric or dollar predictions are made for efficiency or effectiveness, it will reflect on the manager if these figures are subsequently shown to be inaccurate. Managers should not hide such forecasting errors but should investigate and understand why the differences have occurred to enable far more accurate forecasting in the future. Forecasting in these two areas can provide very powerful reasons or arguments when seeking approval for particular technological implementations. The refinement and honing of this process only serves to make the arguments more powerful.

Managing

Organisations should manage their acquisitions rather than just buy products. This means they should know and understand why the technology is being acquired and that they should plan their acquisition to ensure successful implementation.

The best way to plan any acquisition is to know intimately the area for the proposed change. Without this close understanding and knowledge, there is a very high likelihood of overlooking issues or introducing unworkable procedures. This is true not only for the subject area of this paper but for all areas of management. It is important to consult widely—end users, management, support staff, unions and external stakeholders. These practices are particularly important when acquiring technologies.

Acquiring Knowledge

The paper has addressed the acquisition of equipment or services by briefly touching on some of the issues. The question of how to acquire knowledge from our agreed definition is yet to be addressed. The following introduces some of the mechanisms that can be utilised for this process. Before addressing them, however, it is important

to consider the matters discussed above, by implication, with respect to hardware. These apply equally to knowledge acquisition.

Existing staff can be trained, and there is an expectation that this be carried out in the present industrial environment of award restructuring. There are many ways of training staff: from formal courses to internal discussion sessions conducted by individuals with a watching brief on a particular subject area. Another often-used method of acquiring knowledge is the use of consultants and the inclusion of clauses for technology transfer in their contracts. The problem with this procedure is that organisations tend not to evaluate the effectiveness of this transfer of skills and information. Properly managed, this is a useful way of acquiring otherwise unobtainable or difficult to acquire expertise.

During the 1980s, various agencies have introduced staff exchange programs (similar to the universities' professional experience or study leave programs of the past) to gain some benefit from the infusion of new ideas, skills and procedures. Law enforcement agencies seem to have been loath to adopt such programs with organisations other than like-bodies because of perceived uniqueness of their 'industry' or because of potential difficulties of security and other issues. If these issues are recognised and the programs are designed to accommodate both agency and individual needs, then there are many opportunities for law enforcement agencies to acquire knowledge in a very economical way. Exchanges should be in both directions and should include private industry, other government departments and tertiary institutions. Of course, the exchanges with other law enforcement agencies should be easier than those currently in existence.

Any staff exchange program should have clearly-stated objectives for the staff member and both organisations concerned. There should also be an agreed and predetermined methodology for sharing or distributing the acquired knowledge after the staff member has returned to normal duties. An organisation's staff is almost certainly their most valuable asset and yet there is a reluctance to commit money or time to the maintenance of this asset. It would be considered irresponsible for any manager to spend as little on vehicle or computer maintenance as is spent on staff.

The experience of the Queensland Police Service in two programs may open opportunities for other jurisdictions to experiment or develop further. In 1991, the Graduate Research Program has three post-graduate students undertaking research for higher degrees in areas of particular interest to policing. It is expected that this will grow to an ongoing activity for approximately ten students. The range of students is from Honours through to PhD and includes diverse programs such as the analysis of microdots of ink for document examination purposes and digital signal processing. The degree of support by the Queensland Police Service varies from the provision of laboratory materials or an environment in which to work to full salary and laboratory equipment. These programs not only provide leading-edge technology to the Service, but also enhance to a significant degree the perception of the Service as an accountable and professional body.

Scholarships and awards can play a useful role in encouraging individuals within an organisation to pursue excellence in their particular field. To harness and direct the hopes, interests and energies of its staff to the same objectives as held by the employer enables a synergy to be achieved that is not otherwise possible. Time spent in encouraging outside bodies such as newspapers, industry and educational institutions to provide for scholarships and awards is worthwhile. Both the agency and the organisation benefit, as

well as the participating staff. A good example is the annual award by *The Courier-Mail* (Brisbane) for overseas travel and study by a serving police officer.

This paper has not been portrayed as academically complete but rather a distillation of some ideas concerning aspects of technology acquisition that are either ignored or inadequately addressed. The concept of total openness and analysis of the results of that openness are commended to the reader.

Peter Bray
Consultant Software Engineering
South Australia

TECHNOLOGY IS INCREASINGLY HAVING AN IMPACT ON THE WHOLE AREA of crime and policing, and many organisations and individuals are looking for policies and techniques to deal with this. The aim of this paper is to table some checklists and principles that can help in reducing the impact of technology on crime.

There has been ongoing development of high technology systems in the military or defence applications domain for many years, and there are many parallels with the law enforcement area. Principally:

- there are sometimes intelligent hostile forces and innocent parties;
- there is employment of continually improving high technology;
- there are large disciplined forces with a wide range of skills and training who have to interact with all this technology; and
- there are complex and competing organisations engaging in operations that depend on high technology systems and that are also required to support that technology and the people who use it.

Many other derived parallels could be cited, but the point is that, just as the pitfalls and difficulties have much in common, so too the techniques to deal with them have good cross-applicability.

This paper will first address some methods, issues, and strategies that are vital to successful technology acquisition and its ongoing successful management. Next, it will review the types of concrete applications of technology that can be presented: those of a hostile nature (available to the criminal element), and those of a helpful nature (available to law enforcement agencies). Finally, this paper will outline some prominent legal and political considerations that will inevitably surface with the increasing reliance on technology, and particularly information technology (or computers).

The Acquisition Process

The most important material in this paper is in this section. Some concepts and principles useful in the technology acquisition process are outlined.

Off-the-shelf versus custom-built

There is a trade-off between using off-the-shelf equipment or technology as opposed to developing a custom-built technology. A completely custom-built system may take new ground and do so more thoroughly and even more efficiently than an off-the-shelf technology, but at greater initial development cost. An off-the-shelf approach presents lower technical risk. Ideally, a compromise occurs, with an off-the-shelf technology tailored to suit and integrate into existing procedures, logistics, and training.

In-house versus contracted development

Another trade-off exists between in-house (own organisation) development and development that is contracted out. If a technique is developed in-house more job-reward opportunities are created. However, if the technology is developed in-house it is generally easier to lose control of costs and schedules, and lose sight of the vital requirements as opposed to the superfluous frills, resulting in delayed implementation of a balanced product. The technology may never be totally finished and the organisation's infrastructure may never catch up.

If, on the other hand, technology development is contracted out, it must still be managed carefully to contain costs and schedules, to protect the investment, and to ensure that what was bought is provided. The emphasis now becomes one of a careful containment of the scope of the task by one party (the developer) and careful checking

that the scope is fully-implemented and that progress and payment are audited and in step by the other party (the client).

Cost benefit and funding issues

What it costs: Technology done properly is expensive, but is then useable and supportable. The disciplines to make sure of this—in terms of logistic integration, requirements being met, training programs addressed, documentation consistent and accurate, testing systematic and thorough, and systems being safe and fulfilling purpose—cost money: much more money than the raw engineering and research that, on the face of it, can produce the basic tool. But it would otherwise be a basic tool that very few can fix, no-one can use, may be unsafe, may not do what you really need it to, and will be very difficult for anyone else to improve.

Funding options: With high costs come a need to be innovative in our approach to funding. Governments and beneficiaries such as insurance companies can help with funding and proceeds the technology may generate can be used to offset the expense of development. A project may be either a fixed-price contract or a level-of-effort contract. Because defined scope is difficult to manage unambiguously, the former is more popular these days.

Level of effort: The level of effort when deployed must be carefully considered at the outset when arranging funding. If too low it may just train criminals to deal with it. If too high it may not give commensurate benefit or completely displace the crime.

Cost benefit: Cost benefit estimates can make an expensive project seem worth it.

Expenditure control: Expenditure control is particularly important in a project with a development phase. Work breakdown structures, milestones, and measures of progress need to be identified and quantitatively assessed before a payment regime is agreed. Be wary of biased weighing that aims to achieve 90 per cent of the payments for 50 per cent of the work. Once work is proceeding, make sure that progress audits confirm claims.

Vesting: Protect the investment in long and expensive projects with gradually reduced financial guarantees from third parties (like banks).

Reliability and sensitivity issues

At the outset, required reliability and sensitivity need to be understood and agreed upon. At the end, the users must also grasp this or the technology will be misused.

Functional requirements

One of the most important principles in dealing with technology applications is that development is started and finished with the functional requirements of the application foremost in mind: that is, what is and is not functionally required and just how these requirements will be met is understood and agree upon. For example, when designing a car, it is intended that the car will hold so many people, run a certain distance on a specified amount of fuel, have a life of 'x' years, reach a certain speed, corner with a certain level of stability, and cost a specified price. It is not specified at the outset just how the dashboard in this car will look, but it is intended that it will be ergonomic, have the most-used controls nearest to the limb which will operate them, and not hurt the operator.

Generic requirements

In addition to the specific application-oriented functional requirements there will be others that make sense in a life of system context.

Robustness: Systems must resist damage: more or less depending on the harshness of the expected site.

Resistance to counter-measures: Systems should not be readily defeated by counter-measures.

Maintainability: Design, quality, supporting documentation, pre-procured spare parts and so on should make systems maintainable.

Human safety sensitive: Systems should be safe for users and bystanders.

Re-useability: Systems should be useful in other contexts.

Military standards approach

This paper will now return to the military model for insight into how to go from here. There are many international and national standards governing hundreds of aspects of technology development and integration, and they are invaluable assets in management of technology acquisition. However, it is easy to lose the forest in all the trees. Let us now appreciate the forest.

Phased development: Even off-the-shelf technologies require a phased approach because they must suit and dove-tail into your organisation. These phases are delimited or separated by reviews:

Reviews: Formal reviews evaluate the preceding phase and approve the current position as a satisfactory point of departure for the subsequent phase. The conduct of reviews needs to be agreed (often in reference to a standard). There may also be internal reviews within phases conducted within the development organisation.

Phases: Examples of phases are: requirements definition, design, development, test, and integration. Documentation developed during such a phase is usually frozen or 'baselined' at the end of such a phase.

Consistent documentation: An overall aim is to have consistent documentation between the documentation from each phase with that of other phases and indeed with the end-products themselves. This is achieved by a set of formal processes called configuration management. The management of change is a vital aspect of this: whether the changes are enhancements that modify baselines or just corrections. *Configuration Control* is a set of methods to help in this documentation and, very basically, it helps to identify just what changes have gone into a given version of a product or documentation. *Configuration Identification* helps identify the exact hierarchical breakdown of the whole product and relates it to its documentation.

Quality system

People are only human and, no matter how organised a development method is, both people and their tools may be in error. A quality system is there to make sure that the development method is in fact applied and to fix things if it is not. Very often, an accredited quality system is mandatory if an organisation is to be trusted to undertake a development project or even to apply and integrate a technology. This is particularly important if lives and/or expensive equipment may be at risk.

Training and formal procedure

Standard operating procedures and training programs are important tools in allowing ordinary people to interact successfully with high technology. They should be developed in parallel with the products from the start of the requirements definition phase. They should also be tested and qualified. Not only does one need to know that the technology will work but that the people will be able to work with it when the development experts are no longer around to help.

Tailoring of standards

International and military standards are available to provide guidance in implementing some of the above principles and they are, in fact, more complex than the simplified outline given here. As can be imagined, standards are expensive to implement in full. However, that is no reason to drop them altogether. Depending on how complex, life-critical, urgent, or otherwise a project is, the need for adherence to standards can vary. The proper course is to agree prior to contract award on a tailoring or subset of the standards that are to be adhered to.

Progress auditing

Throughout any acquisition there is a process of payment to agreed schedules. Progress audits are a combination of claims and certificates of progress against the plan plus interviews where work and documents are inspected to check those claims. One difficulty in this audit system occurs where contracted work is subcontracted. Invariably there will be situations where the subcontracted breakdown of scope does not quite match the contracted one or the sequence of work differs.

Functional audit

The end-product must be checked as fulfilling all the functional requirements properly. Consequently, there needs to be traceability to them from the formal tests in evidence.

Commercial management

Commercial management of the progress of a contracted project is no small topic in itself. It may be helpful, however, to give some examples of the commercial effort that must be undertaken.

Cost and schedule control systems: To support progress audits and payment, some form of cost and schedule control system is needed.

Scope commitments and concessions: In meetings and in correspondence between the contractor and contracting agency, whether to resolve issues, interpret specifications, or interface systems, we must always worry about scope. Implicit commitments or concessions may be given that impact on the formal scope of a task, and the consequential impact on cost and schedule may be quite horrendous.

Alignment of deliverables: In most technical projects there is an obligation on both parties to deliver items of equipment, information, and services to the other. Quite often these must be obtained via other contracts. It is important that the dates, quantities, and specifications match and this does not happen by itself.

Scientific approach to new techniques

One further insight that should be tabled is that a scientific approach should be applied not only to new technologies but to new techniques.

Diversity and innovation versus standardisation and re-use: New techniques may be viewed as departures by some from standard procedures but if managed properly they can advance things. Viewed as controlled experiments they are justifiable provided two things happen:

- Independent Quantitative Assessment: When one is informally convinced that a technique works, the technique should be independently and quantitatively assessed by independent parties.

- Document and Franchise: If proven useful then it should be re-packaged so that others can use it without the personal presence of the inspired but mortal team leader. In other words it should be formally defined so that it can be franchised.

Targeted training and documentation: An adjunct to this realisation is that the documentation where possible should take into account the level, sophistication, and interests of the users of that documentation. Will a document be used by maintainers, users, test teams, management, the public or combinations?

The Acquisition Checklist

Some delegates may be surprised or even intimidated at the diversity of issues and principles just outlined. Admittedly, a lot of the points outlined in this paper seem somewhat abstract until one begins to manage a real project or to acquire and implement technology. Then this checklist may become useful and one can either:

- get better resolution by reference to a wealth of standards and/or;

- get less resolution (simplify things) by tailoring the management requirements.

This paper will now examine the sorts of technologies that police work might encounter.

Technology-Based Crime

The point in outlining technology-based crime is so that it can be systematically countered. This paper does not intend to be exhaustive, but merely to introduce a few principles. Countering these ought to be one more functional requirement that we put on our technology systems.

Computer crime

Because of the mystique surrounding computers, all too often the level of protection against crime involving information is insufficient. It falls into several areas:

Traditional fraud: The audit checks and balances implicit in the requirements placed on financial systems application software are all too often relied on to counter the threat of fraud in the computer environment. The hosting environment and technical administration is just as important and needs to be explicitly managed.

Data sabotage: Data sabotage may aim to perpetrate data loss or, more dangerously, insert mis-information. Protections against this are as in fraud, but the procedures need also to focus on controlling the quality and accreditation of data as entered normally.

Data theft: Data theft has the potential to not only disrupt the viability of enterprises, but even entire economies. If information has great value, it will be targeted.

Criminal manufacture

Counterfeit: Counterfeit money in the age of the colour photocopier is an obvious and hard-to-detect criminal opportunity. Technology, however, makes accessible a far wider scope of operation for counterfeiting than merely traditional targets of money or art.

Weapons: Technology in weapons development is a two-edged sword. Modern materials and explosives create particular headaches. Information technology initiatives in identifying, tracking, controlling and interdicting materials, and methods of manufacture and mandatory standards for storage and safe-keeping are broad measures for which responsibility and funding need clarification at the political level.

Cultivation: High technology illumination and irrigation machinery and even nutrients are the tools of both criminals and bona fide horticulturists. They are, nevertheless, factors in the information correlation game that is increasingly played to detect such crime.

Organised counter-policing: The 'what-if-I-were-them' mind game is one which should be played now and again to make sure that criminals are not unwittingly helped.

Communications encryption: The more organised criminal elements no doubt employ communications encryption and discipline, and it is not intended to explore what we can do about that here. What will be said, however, is that levels of classification are needed so that enforcement organisations can function. If any officer encounters a measure, then procedure has to be available, and to some extent that procedure should be an unclassified interface into a classified area of operation.

Police identification: The more organised criminal elements are also liable to attempt systematic identification of law enforcement officers. What is to be done about that?

Communications interception: Criminals routinely attempt to intercept police communications and as all law enforcement agencies understand this, discipline and technology are used to combat the intercept threat. Law enforcement agencies, however, are only human. and technology is forever being overtaken. Ongoing quality programs need to address this special issue.

Technology-Based Policing

Computer mapping and statistics

This application illustrates an important principle: all the complex information in the world is of little use if system users cannot conveniently access relevant data. Pinning statistics onto a geographical map brilliantly makes complex information practically useful.

Movement planning

Resources available are never enough. Powerful deployment strategies can make the most of our assets and concentrate them when and where most needed.

Intelligence

This paper will make several points on this topic but will not go into detail. The main point that should be made is that technology continues to present new and improved solutions and that military strategies suggest tactics for these available technologies. People in the field need less classified interfaces into these resources in functional requirement terms. Classify the means and techniques, but if one does not know technology is there it cannot be used, and the more technology is used the sooner ground is taken in the fight against crime.

Databases

Managers do not need to become involved in the intricacies of the databases themselves but do need to bear in mind five issues. Databases must:

- be requirements-based; it is important that we know what is to be achieved with information kept;

- be accurate and record its reliability. It is both scientific and just that the level of reliability of data be recorded along with that data. If maps on a system drawn by Matthew Flinders are kept together with maps created with the aid of the latest technology, the most accurate maps ought also to be recorded;

- facilitate date exchange and standardisation. It is important that every agency not re-invent the wheel each time but that the technology is re-used and that data can be exchanged efficiently if permitted by policy;

- permit correlation processes. The database engines chosen need to do more than hold information; they need to be able to conduct correlations and reconciliations without personnel directing such activity; and

- be security conscious. The databases must themselves be secure against hostile interests.

Automation

Camera Image Processing illustrates one area of automation being put to efficient use. There are many more.

Digital communications

Digital communications are revolutionising operations, but is there effectiveness being measured?

Electronic parole

Electronic parole has potential economic benefits but just how foolproof is it?

Forensic techniques

Some innovative and powerful techniques are appearing in this prestigious field, but how reliable are they in the context of the organisations employed, and do users know how to go about getting the services? Computer Aided Appearance Reconstruction and DNA typing, for example, are two novel techniques.

Mass media

Mass media involves two different sciences or technologies:

- the technologies of delivering information; and

- the techniques of mass persuasion.

How do these impact on policing? Let us look at a problem and the opportunities. A problem is that both news and drama suggest techniques for criminal action to criminals. An opportunity is that advertising dollars might get the public to help with investigations and that those tempted be encouraged to change their ways.

Legal and Political Considerations of Information Science

In conclusion, a few legal and political issues, relating to the use of computers in crime and policing might be worth tabling.

Large scale data misuse and the economy

Just suppose that undetected data theft from law firms and financial houses is rampant. What contribution might that have made to the recent collapses and economic woes? What should be done and who should do it?

Police role against computer crime

There *are* technical defences. What role should law enforcement agencies play? The problem is that much of the earlier-mentioned crime would, by its nature, be going undetected and therefore unreported. Nevertheless, the social consequences of such crime can be catastrophic. Funding of proactive strategies to cope is a political question but is one worth pursuing. Formal standards, accreditation processes, and mandatory compliance in enterprises vital to the public interest—such as banks and brokers—will be necessary in the longer term. There is, of course, another side when an enterprise itself may be on the wrong side of the legal fence. Search warrants for information should be backed by an understanding of how to penetrate computer security.

Political criminality—the definition can change

Think back to Nazi Germany or recent communist USSR: what is deemed to be criminal can change dramatically and not always for the good.

Changes in political systems: as databases and correlation processes are established in the public interest, be aware that things may change just as dramatically where you live.

War and invasion contingency: at very least, war and invasion contingency should be planned for.

Cultural determinants: as cultures evolve and ethnicity balances alter, the determinants of what is appropriate and in the public interest may also alter.

Rights to privacy

In 1991, there is a public tension between rights to privacy and public interest. As in most things, a realistic compromise, sets of rules, and a degree of tolerance will most probably evolve.

Operational security versus political oversight

A final issue is that operational security and political oversight are not necessarily compatible. A middle ground that achieves both missions needs better definition.

Government role models

Technology has afforded governments at all levels with bureaucratic opportunities to mislead, misrepresent and defraud the humble citizen who is all too often bewildered by technology. For example:

- insurance companies required to notify withdrawals from superannuation funds but not deposits that would allow roll-overs to be automatically correlated. Instead, complex forms must be lodged, or one is taxed;

- new parking ticket machines introduced at the same time as cryptic road signs; and

- Financial Institution Duties (FID) deducted for transfer between accounts accompanied by pensioners being pressured into moving money into high interest accounts without cheque facilities.

Politicians and the heads of law enforcement agencies have a responsibility to be proactive in preventing trends in the direction of sanctioned government misrepresentation or fraud. They are role models and too many are already alienated—or has nobody noticed that someone must be buying the goods from the one-in-six households broken into each year?

Conclusion

This paper has covered a lot of ground in a short time: from methods and considerations in managing the acquisition of technology, to checklists of technology applications and contentious philosophical issues. All should stimulate some debate and questions on the management of technology that is being acquired by law enforcement agencies.

LAW ENFORCEMENT ACCESS NETWORK

Peter Roberts
Attorney-General's Department
Canberra
Australian Capital Territory

THIS PAPER OUTLINES THE LAW ENFORCEMENT ACCESS NETWORK (LEAN) proposal recently announced by the Commonwealth Government. The proposal arose as a direct consequence of the Commonwealth Government's acceptance of the recommendations in 1987 of the white paper entitled *Review of Systems for Dealing with Fraud on the Commonwealth* (Australia 1987). A description of the Commonwealth's campaign against fraud is provided at Appendix A.

Concept and Aetiology

Recommendations 14 and 15 of the *Review of Systems for Dealing with Fraud on the Commonwealth* (Australia 1987) deal with the computerised use of corporate affairs records and land data by Commonwealth agencies with law enforcement functions.

The Attorney-General's Department, in assessing the most effective way of meeting the recommendations of the Review of Systems for Dealing with Fraud on the Commonwealth and providing a data analysis facility which would meet the broader law enforcement needs of the Commonwealth, has given regard to the following factors:

- the Australian Securities Commission and the land information functions of the state and territory governments have reached differing levels of development of the computerisation of their records;

- no existing state or territory facility can meet the needs of Commonwealth agencies for computer analysis of their own individual state or territory records, leaving aside national records;

- the Commonwealth needs to take advantage of the latest developments in the hardware and software technology for searching, collation, interrogation, data matching and case manage-ment of large amounts of data; and

- the Commonwealth has to meet the highest standards for the protection of the security and privacy of the information it handles.

The basic notion underlying LEAN is that information technology has reached a stage of development capable of handling data of dubious quality for law enforcement and fraud protection purposes. There are several key elements in the proposal that are essential to understanding its purpose. These are:

- a central computer facility operated by the Attorney-General's Department holding the publicly accessible databases;

- taking data from suppliers without modification;

- gateway access to terminals in the user agencies; and

- a capacity to use sophisticated search and investigation techniques across the available databases.

The Attorney-General's Department is of the view that LEAN will assist the Commonwealth in protecting its revenue and enhancing its law enforcement capability. There is a strong argument that, at a time of economic restraint, the Australian taxpayer is becoming increasingly intolerant to the loss of revenue resulting from fraud, waste and abuse. The use of data-matching techniques and exchange of information between government agencies has, in the past, been a matter of keen public debate. However, a balance needs to be struck between protecting the public purse from the depredations of the dishonest and the privacy of the individual. This issue is discussed in a later section of this paper.

A six-month pilot was conducted between February and August 1991 to ascertain whether the LEAN concept is viable and to assist, if possible, in estimating the savings more accurately than has been possible in the past. The pilot used corporate affairs records and land data from one state, to be accessed by six Commonwealth agencies with law enforcement or public revenue protection responsibilities. The participants in the pilot were the Australian Federal Police (AFP), Australian Tax Office (ATO), Department of Defence (DOD), Department of Employment, Education and Training (DEET), the Office of the Director of Public Prosecutions (DPP) and Department of Social Services (DSS). During the pilot, DSS used its own system to interrogate the data acquired through LEAN and will continue this practice with the permanent facility.

The pilot indicated a range of potential uses for the LEAN facility. These can be grouped as follows.

Investigation

Law enforcement is moving rapidly into the area of financial and company affiliations. LEAN enables users to get behind the 'corporate veil' using sophisticated analytical capabilities.

Checking of contractors

Proactive fraud control requires public sector bodies to better understand the nature of the corporate entities with which they contract. LEAN provides a valuable insight into company affiliations.

Benefits control

Many Commonwealth benefits programs are assets-tested. Ownership of property is one of the most crucial elements of assets tests and LEAN will provide the capacity to check client statements quickly and cheaply against a national database.

Assets tracing

By analysing both companies and land information together, LEAN enables beneficial interests in property to be traced. This is particularly useful for enforcing Proceeds of Crime legislation.

Taxation

The companies data and land records were found to be of particular relevance to the taxation collection function.

All agencies which participated in the pilot have indicated their intention to participate in the full LEAN system.

LEAN will provide a *value added* facility which builds upon currently available data by assembling it in the one place, providing on-line electronic access, enabling the two databases to be searched concurrently and allowing the data to be entered through a multiplicity of fields. The Attorney-General's Department does not see LEAN replacing any existing facilities, rather it will add to their effectiveness and usage.

Functions and Approach

The user agencies, in consultation with the Attorney-General's Department, identified the following needs for LEAN:

- to provide searching, collating and analytical capability enabling definitive matching of ownership records of property assets, with data provided to, or obtained by, Commonwealth agencies for the execution of law enforcement responsibilities. Some of the information may be obscure, incomplete, or otherwise presented to conceal true ownership or identity;

- to enable the investigation of such information, together with other data owned by the Commonwealth agency, by annotation, sorting, collation, indexing, cross-referencing, linking, extraction into separate files with other relevant data, financial analysis spreadsheeting and output in other appropriate manner; and

- to facilitate the preparation of prosecution material, including organisational charts, identifying how participants and companies interrelate, scheduling documents according to witnesses, chronologies of events showing major relevant items such as dates of appointments, major transactions, flow charts, and so on.

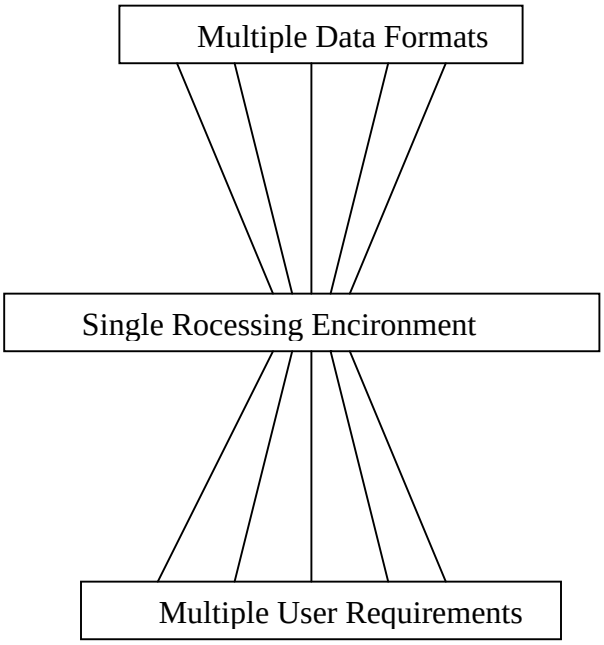
One of the major functions of LEAN will be to bring together data from a variety of sources which have a variety of formats and actual data elements into a single facility which has a common set of front-end inquiry and analysis procedures. While the introduction of the Australian Customs Service (ACS) corporate affairs information system will provide a single, national source of data, the electronic land data systems in the various states and territories will continue to be at different levels of comprehensiveness and sophistication. Some are highly structured, while others include some or all of their information in unstructured, 'free text'. Some have all relevant data in a single system, while others have it spread across multiple systems and holding agencies. While LEAN will always be dependent on the agencies providing the data for its accuracy and comprehensiveness, LEAN will make the structural variations transparent to users.

This assumes successful negotiation of a number of constraints. For example, there would be privacy implications for LEAN to change the actual content of the data by using some sort of 'data scrubbing' process. While scrubbing might be used, its output would therefore need to be stored in addition to the original, requiring additional computer memory and further complicating the searching process, as the original version may in fact be valid and cannot simply be ignored. As well, if a structured database solution is to be used, the extent of reformatting must be kept within a reasonable limit, yet result in a single format while accommodating the wide variety of originals—a formidable task. The need to merely distinguish the different parts of an address, when the original database includes everything from flat number to suburb in a single field and in varying order, presents an almost insurmountable barrier.

At the same time, the various agencies using the data will have differing levels of complexity in their requirements of the LEAN system. These will also vary within user agencies from inquiry to inquiry and from analysis to analysis. In fact, one of the few things that is certain is that the extent to which users will want to use and analyse the data provided through LEAN is not known. Yet LEAN must have the capacity to respond to users' needs. All this must be achieved by a system which is user-friendly, not daunting, cumbersome and inhibiting. Figure 1 presents a graphical representation of the LEAN approach.

Figure 1

The LEAN Approach



The two most salient features of the LEAN system will thus be its flexibility and adaptability. To accomplish them without constant intensive human intervention requires an extremely advanced processing system. The pilot has demonstrated the feasibility of the approach and that at least one currently-available computer system is adequate to the task.

Data currency

LEAN will be implemented with initial 'snapshots' of selected fields from provider agencies' complete databases. In order to satisfy the needs of the majority of user agencies, the data on LEAN must be kept as current as possible. The system will, therefore, receive daily updates (where available) of all changes from data providers. These updates will be maintained in an aggregate 'change file', which will be searched in parallel with the main file. Thus, an historical information base will eventually develop on LEAN (most holders of land data maintain only current information on their electronic records). User agencies will increasingly be able to perform historical inquiries and analyses, thereby enhancing their investigations. This is of particular importance to agencies such as the ATO whose interest is in the status of assets one or two years previously and in their transition (for example, in value) over time.

The extent of the on-line historical coverage of LEAN has not yet been determined. A number of factors are still to be considered, not the least of which is the capacity of the chosen computer platform. A near-line capability would meet the dual requirements of archiving and accessing data quickly.

Still, LEAN will never supplant the data providers as the official holders of the data. Although the information on LEAN will be always the most recent available, user agencies will be required to, and have agreed to, obtain official records directly from the originating agencies prior to commencing any formal legal or administrative proceedings.

Integration with current user systems and networks

The LEAN pilot involved the use of dedicated terminals and data lines to all users. All user agencies involved in the LEAN pilot and others who have committed to participate in the full LEAN system have indicated that they will link their networks to the LEAN facility. This will enable them to more easily maximise and manage access to LEAN—using software security controls rather than physical arrangements to limit access. It will also ensure that appropriate users will have LEAN immediately to hand, via their own terminals and familiar menus.

Cost-effectiveness

It is evident that the new system will be cost-effective for user agencies. Previously, the costs, in terms of search fees and staff time, have been such that such searches were kept to a minimum by most agencies. As well, without familiarity with the peculiarities of each data provider's system, the effectiveness of searches has often been in doubt. LEAN will alleviate both of these deterrents to effective investigation. As noted above, users will still need to go to the originating agencies for official documents, but only in those cases where it is known that they exist and the decision has already been made to use them. This will reduce wasted effort and expenditure considerably. Also, in providing a single, user-friendly access point and infrastructure, LEAN will make searches less onerous and unpredictable.

Of even greater importance is the fact that no previous land or corporate information system has supported the types of analysis available on LEAN, not even for a single database. LEAN will, therefore, provide capabilities to law enforcement and public revenue protection agencies not previously available *at any cost*. The returns from such new capabilities are only beginning to be predicted, as experience has been gained from the pilot. Even then, the pilot has only involved the data from one state. The full system will not differ from the pilot only in magnitude. It will be altogether qualitatively different.

Lastly, the nature of LEAN as a shared facility, in itself, presents a major cost-saving to the Government. The only alternative, aside from having no such system (which is increasingly becoming thoroughly unacceptable), is for individual agencies to develop their own. Assuming this would even be possible for the smaller agencies, the wasted duplication would be totally indefensible, especially in the current fiscal reality. The fact is that many of the current and future user agencies would be unable to justify even a basic inquiry system in their own rights.

Security and Audit Functions

The system is required to have a high level of security to protect its data, information and operational integrity from both external and internal attack aimed at breaches of privacy or security, or at achieving any malicious intent. The minimum mandatory requirement placed on LEAN is to achieve a centrally imposed security level. This will be equivalent to Level B1 on the USA Department of Defense security scale and will enforce security as required without relying upon voluntary good behaviour by either the users or the applications software they use. As a minimum, the following main security features will be included:

- ability to mark each entity (user, file, data, item, disc, partition, and so on) with a specific level of sensitivity;
- ability to determine which users are permitted access to what data and programs, and to what level of sensitivity;
- ability to ensure that untrusted application code or data operating in high sensitivity environments cannot violate the determined levels of security (that is, can detect 'Trojan horse code');
- ability to label both printed and displayed information with its appropriate security classification;
- comprehensive audit facilities;
- protection of discarded data;
- enabling of restrictions on data to be set for specific functions (read, write and delete) at differing levels according to various possible groupings, including grouping by:
  - department, section, user and user group;
  - network, sub-network, terminal and terminal group;
  - library, file, record and data item; and
  - data value (specified by individual's files or by type of information).

While general LEAN usage will be monitored centrally, primarily for system management and accounting purposes, individual user agencies will be responsible for monitoring the specific activities of their staff members. Some agencies have decided to maintain highly detailed audit trails of their use. Even though the actual LEAN data are publicly accessible, each agency's own data are not, and the reasons for such a high level of vigilance are obvious. By supporting a high level of security control and auditability, LEAN will largely ensure that it is not used inappropriately.

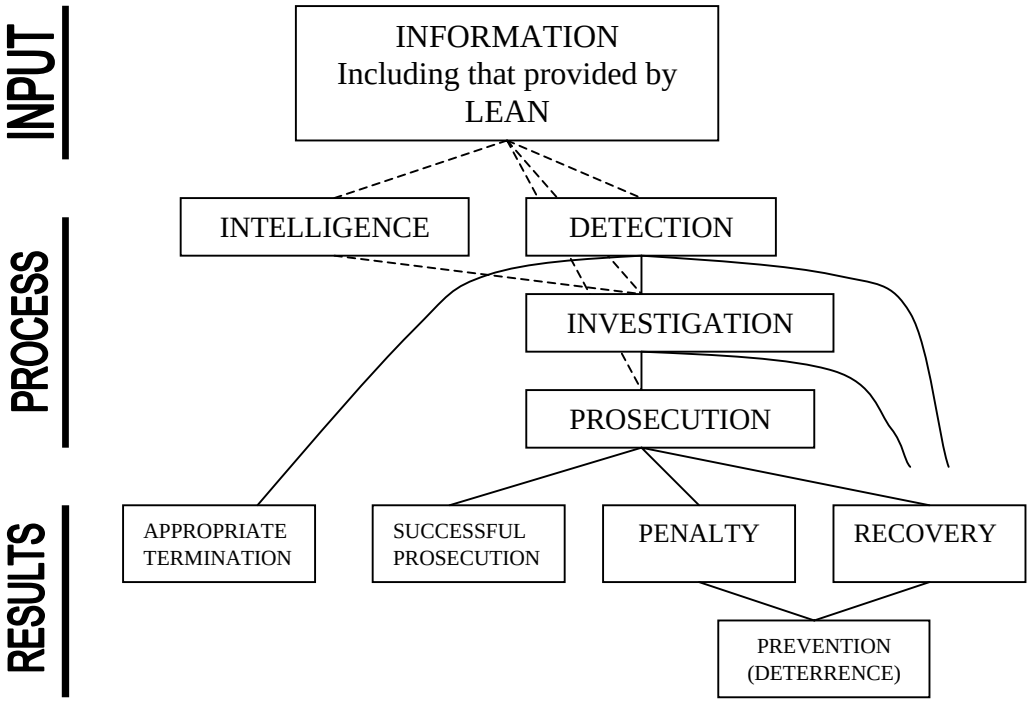
Impacts on Law Enforcement and Protection of Public Revenue

It is quite apparent that, in conjunction with other sources of information and both traditional and developing investigation techniques, LEAN will have major impacts on public revenue protection and certain types of law enforcement efforts. The former will benefit directly from the ability to identify and evaluate assets, resulting in both more appropriate distribution of benefits and more effective revenue generation. As well, the effects of LEAN on law enforcement will permeate its whole process.

As Figure 2 shows, the LEAN information will feed directly into each stage of that process. As well, the information obtained and analysis performed at each stage will also benefit subsequent stages. Additionally, though not within the mainstream of the central law enforcement process, criminal intelligence is nonetheless of major importance in supporting it. In fact, it is in the intelligence arena where much of the most thorough analyses of information such as that provided by LEAN occur, the results of which ultimately benefit case-specific investigations.

Figure 2

Law Enforcement Activity Path as Affected by LEAN



– – – Information Flow ———— Process

LEAN's contribution to the law enforcement process will undoubtedly affect each of its possible results. The number of cases resulting in unsuccessful prosecution will decline, with more resulting in success ('penalty') or appropriate termination (for those which should not proceed). Termination decisions should also be made earlier in the process, thus allowing resources to be more effectively allocated. Recoveries of

proceeds of crime should also increase. The ultimate outcome of more frequent and increased penalties and recoveries is prevention, as the likelihood of financial gain from criminal activity is reduced.

The Privacy Issue

The primary issue relating to LEAN is the public availability of the data. Upon payment of a fee, any member of the public can obtain it, either in manual or electronic form. LEAN will operate to provide a service to Commonwealth users with law enforcement and protection of revenue responsibilities in a way analogous to a library, with users accessing the data using sophisticated search facilities.

Other than accessing the two publicly available databases, there will be no exchange of data on the facility. Nor will it be extended to other databases without specific government direction.

It is recognised that, in the planning of a facility such as LEAN, it is of utmost importance that appropriate protection for privacy be included. In this context, the sort of issues which have been identified are:

- stringent security barriers will need to be built into the system to preclude any exchange of data, other than through accessing the land titles and corporate affairs databases;

- the facility will need to be capable of restricting access to particular persons by virtue of a user identification, with the ability to log each access and record it for audit purposes; and

- participating agencies will need to develop auditable procedures for the safeguarding and proper disposal of the results of accesses to the facility.

The Attorney-General's Department considers that the requirements set out above will provide adequate physical safeguards for privacy for all data held or processed on the system.

In the light of the public availability of the common data being contemplated for LEAN, the Department considers that the system's development and operation falls within the law enforcement and protection of public revenue exemptions to Information Privacy Principles 10 and 11 of the *Privacy Act 1988* (Cwlth). However, the Department is currently proceeding as if LEAN were not exempt, in order to ensure that individual privacy is not unnecessarily compromised. Should agencies, having obtained information from LEAN, use it in conjunction with personal information from their own files, they would be subject to the Information Privacy Principles in the Privacy Act.

The Attorney-General's Department has consulted the Privacy Commissioner on the project and invited him to participate in the formulation of the necessary privacy safeguards.

The Fraud Policy and Prevention Branch will continue to consult with the Privacy Commissioner on this and related matters.

Current Status and Plans

The LEAN pilot ended in mid-August 1991. An evaluation was conducted, based on data collected and the experiences of the users during the course of the pilot, and completed in September. The evaluation concluded that the LEAN approach had been proven.

A proposal for the full LEAN system was put before the Commonwealth Government in the course of its budgeting process. Based on the pilot evaluation and supporting representations from all participants, the Government approved the establishment of a permanent LEAN facility in October 1991.

Expressions of interest in developing the LEAN system have been solicited and received from industry. Following government approval, a draft Request For Tender (RFT) was issued to industry for comment. The final RFT is expected to be issued in mid-December for implementation of the system in the first half of 1992.

References

Australia. Review of the Systems for Dealing with Fraud on the Commonwealth 1987, *Review of the Systems for Dealing with Fraud on the Commonwealth*, Australian Government Publishing Service, Canberra.

Appendix A

THE COMMONWEALTH'S CAMPAIGN AGAINST FRAUD

In 1985, the Commissioner of the Australian Federal Police become concerned that there was a considerable imbalance between the demands for attention to fraud against the Commonwealth and the resources available to address that task. That process led to the Review of Systems for Dealing with Fraud on the Commonwealth. The Review reported in May 1987 and its recommendations included:

- to overtly place responsibility for fraud control with the individual agency;
- to ensure that resources available to address fraud were being wisely allocated where the need was greatest;
- to increase awareness of fraud in the service generally, but particularly at the level of senior management and Ministers;
- to improve liaison between upstream agencies (those Commonwealth agencies against which fraud is being perpetrated) and downstream agencies (those Commonwealth agencies responsible for the investigation and prosecution of fraud; such as the Australian Federal Police [AFP], Director of Public Prosecutions [DPP] and the Australian Government Solicitor [AGS]);
- to provide or locate avenues of training for staff at all levels in fraud awareness, prevention, detection and control; and
- to free up the flow of information to law enforcement agencies to enhance their capacity to deal with fraud when it was discovered or reported.

In general, the Review recognised that it is preferable that fraud be prevented in the first place.

In September 1987, the Government adopted the majority of the recommendations of the Review. The two recommendations not adopted (Recommendations number 25 and 26) related to the proposal to amend the secrecy provisions in specific Commonwealth Acts to allow access to information by law enforcement agencies for the purposes of investigating fraud and other indictable offences. These two recommendations are being held in abeyance pending the outcome of a separate review by the Attorney-General's Department regarding the overall issue of secrecy provisions in all Commonwealth legislation.

The Fraud Control Committee

In September 1987, the Government also decided to establish a Fraud Control Committee to ensure that its decisions on fraud were given effect. The Committee comprised the (then) Associate Secretary of the Attorney-General's Department, Mr Alan Rose, the Secretary to the Department of Finance and the Secretary to the Department of Social Security, or their nominees from time to time.

In brief, the Government asked the Fraud Control Committee to:

- identify areas in which priority should be given to improved arrangements for dealing with fraud;
- evaluate risk assessments and fraud control plans;
- coordinate and monitor the implementation of the recommendations of the fraud review;
- facilitate the sharing of skills and knowledge between agencies for preventing, detecting and dealing with fraud; and
- monitor the use of resources required for dealing with fraud.

In announcing the creation of the Fraud Control Committee, the then Attorney-General, Mr Lionel Bowen, commented:

> Implementation of the Review's recommendations and the establishment of the Fraud Control Committee will improve the government's capacity to reduce the present abuse of public revenue and expenditure programs and to deliver its benefit programs as intended, to those most in need (Media Release, 'Fraud Review and Fraud Control Committee', 29 September 1987).

In that second decision in September 1987, the Government also asked the Attorney-General to report back to government on progress in implementing the decision. Two years later he did so. In that report, he told the Government that there had been substantial compliance with many of the elements of the original decision, but there was no question that the task of fraud control in the Commonwealth had to continue and that all agencies and the Attorney-General's Department had ongoing responsibilities.

The Fraud Policy and Prevention Branch

The Government, in considering the Attorney-General's report, agreed that the Fraud Control Committee should be disbanded; however, it also agreed that the Fraud Policy Unit (now the Fraud Policy and Prevention Branch, located in the Federal Justice Office of the Attorney-General's Department) continue with the function of monitoring compliance with the original decision. The Branch has been specifically charged with the responsibility of continuing to evaluate risk assessments and fraud control plans, in consultation with the Departments of Finance and Social Security. The Branch is also required by the decision to refer its assessments and the documents to the Australian Audit Office for consideration as a part of its ongoing audit functions.

As currently stated, the organisational objectives of the Fraud Policy and Prevention Branch with respect to fraud control are:

1. Monitor compliance with the recommendations of the Review of Systems for Dealing with Fraud on the Commonwealth.

2. Enhance the management of Commonwealth resources by:

   (a) improving fraud control through the provision of policy advice to the Government, Ministers and the Executive of the Attorney-General's Department on fraud matters;

   (b) improving fraud control in Commonwealth departments and agencies by encouraging managers to adopt working practices which minimise the risk of fraud through protection of national assets and resources and through encouraging the use of risk management techniques to allocate scarce resources to the areas of greatest need;

   (c) providing leadership, guidance and support to those persons in Commonwealth Departments and agencies given the responsibility for fraud control within the agencies;

   (d) encouraging agencies to improve fraud control through exchange of information on detection, prevention, investigation and prosecution of fraud against the Commonwealth;

   (e) increasing awareness of managers to the opportunities which developments in technology can provide for improving law enforcement and the protection of public revenue;

   (f) facilitating the review process of Commonwealth Departments and agencies for risk assessments and fraud control plans; and

   (g) providing information and comment in public forums relating to the progress the Commonwealth has made in its fraud control activities (Media Release, 'Fraud Review and Fraud Control Committee', 29 September 1987).

The Fraud Control Committee made a decision on how to determine whether the Government's requirements had been met by each agency. It promulgated guidelines for the evaluation of risk assessments and fraud control plans and these were circulated to all affected agencies. As a result, in considering a fraud risk assessment the Fraud Policy and Prevention Branch asks the question:

> Has the Minister been adequately advised of the risk of fraud?

and in considering a fraud control plan, it asks:

> Is a plan in place which identifies for every manager in that agency what (s)he needs to do to reduce the identified risks?

There is no benchmark; nor is there a 'pass' or 'fail'. However, with the experience of reviewing a number of fraud control plans, the branch has identified a number of common elements which are manifested in successful plans:

- evidence of commitment at the executive level to the objectives outlined in the plan;
- existence of a structure to coordinate the agency's fraud control strategy;
- allocation of responsibility for implementation of the various aspects of the plan;
- a realistic timetable for implementation; and
- a capacity to assess performance—undoubtedly the agency will be asked at some time in the future how successful its fraud control plan has been.

Having completed and implemented a fraud control plan does not mean that an agency can put the issue of fraud control aside. The Fraud Control Committee's guidelines require agencies to review their fraud control strategies at least every two years. Implementation of new administrative arrangements has needed to be undertaken in the context of proper fraud control. Technological change, particularly with the introduction of new computer systems, requires fraud control to be undertaken at each stop. Automation can open up new areas of fraud, existing controls may be inappropriate and the vulnerabilities should be addressed in the implementation stage, not after the first major fraud has been discovered.

Virtually all the Commonwealth departments and agencies covered by the Government's decision on fraud control have submitted risk assessments. Forty fraud control plans have been evaluated by the Attorney-General's Department and most agencies are into the first review phase.

TRAFFIC CAMERAS: THE VICTORIAN EXPERIENCE

Michael G. Bourne
Inaugural Director of the
Victorian Traffic Camera Office

Ronald C. Cooke
Initial Appointee to the Office of
Assistant Director
Systems Development
Victorian Traffic Camera Office

THIS PAPER DISCUSSES THE DEVELOPMENT OF VICTORIA'S TRAFFIC CAMERA Enforcement Program which began with the introduction of red light cameras in 1982 followed by the first use of speed cameras in Australia in 1986. The new Traffic Infringement Management System (TIMS©) was the result of this Program.

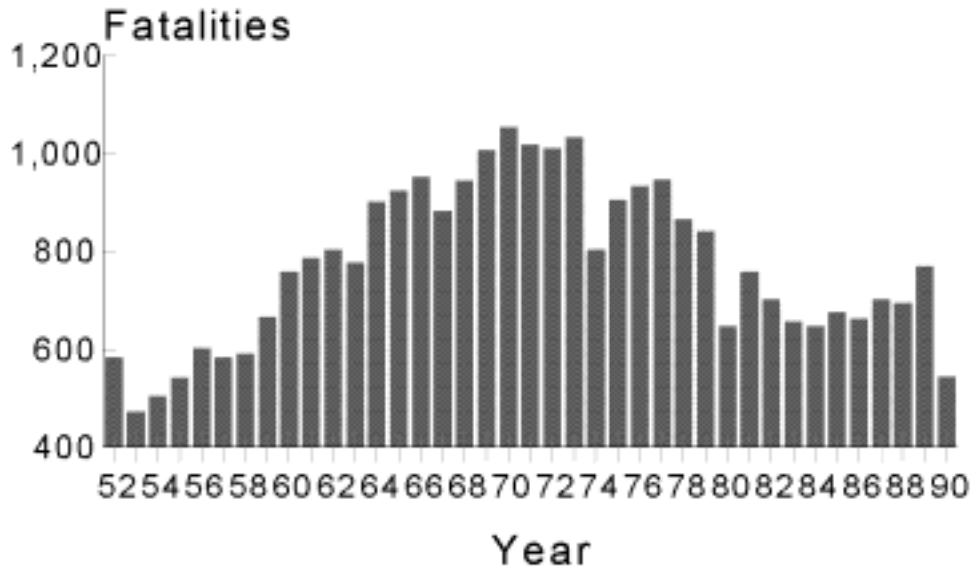
Stop the Slaughter

By September 1989 Victoria had experienced two years of rising road carnage. For the previous twelve months the state had racked up a massive 796 fatalities and this was growing at an alarming rate of more than five additional deaths per month (Victoria Police. Traffic Operations and Support Department, various years). On these figures, Victoria would have experienced in the order of 870 fatalities the following year and, if unchecked, within a few years would have been facing the record levels of the 1970s (*see* Figure 1).

Victoria was not alone. The Australian road toll was then, and remains today, a national disgrace. Yet fatalities are not the only measure of road safety. In fact, of greater cost—especially to the government, and in terms of human misery—are those seriously injured and incapacitated on our roads. Whilst the media focused on the road toll, which was steadily declining during the early 1980s, the number of people maimed and crippled climbed unabated. In 1975 some 18,000 people were seriously injured. By 1985 this had risen to 23,000, and by 1989 more than 37,000 people were

injured as a result of crashes—10,000 of whom were hospitalised (Victoria Police. Traffic Operations and Support Department, various years). It was no time for complacency; but it took a rising death rate for the problem to be recognised (*see* Figure 2).

Figure 1
Victorian Road Toll 1952-1990



It is surprising that this issue remained hidden for so long. The cost of road trauma to the community is enormous. The government has to maintain emergency services, provide hospital and medical facilities, cover accident compensation, and provide welfare and support for the injured. Combining this with the loss in productivity to industry—in the order of 200,000 person days per year—the cost in Victoria alone is estimated at $1.5 billion. In 1989 the Australian Office of Road Safety estimated the cost to the Australian economy of road traffic trauma at:

- $450,000 for each fatality;
- $92,000 for each person with major injuries;
- $10,000 for each person with minor injuries; and

- $1,000 for each vehicle involved in 'property damage only' collisions (Australia. Bureau of Transport and Communications Economics 1989).

Figure 2

Motor Car Injuries and Fatalities 1960–1989

Australia can ill-afford such waste; Victoria certainly could not. Yet even these economic consequences pale when placed against the personal grief and suffering for those involved. Something had to be done! Something big and something more than what had been done in the past.

Identifying the Problem

There are three factors inherent in any car crash:

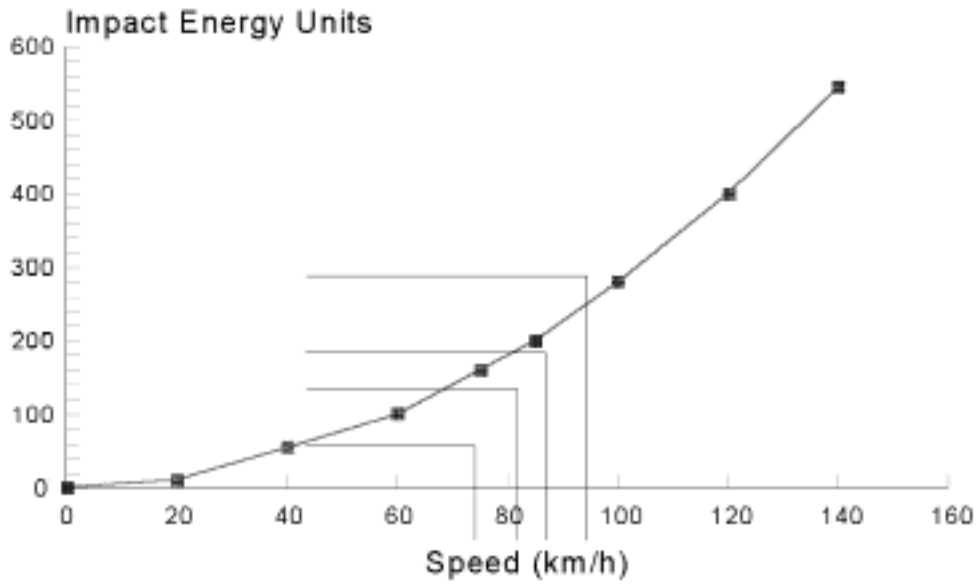
- road conditions;
- vehicle performance; and
- driver behaviour.

The majority of collisions occur because people use vehicles inappropriately for the environment in which they are driving. More than 90 per cent are the result of human error, 35 per cent involve environmental factors, and about 1 per cent arise from vehicle malfunction (Vic Roads 1991b).

Alcohol, carelessness, inexperience and disregard for traffic signals are all facets of the human factor responsible for crashes, but speed was seen as a major contributing element in a large number of the collisions. However, it is not simply velocity that is the culprit; the range of speeds inherent in traffic appears to play a significant role in creating accident situations.

Solomon (1964), Munden (1967), Research Triangle Institutes (1970) and Fildes, Rumbold & Leening (1991) have noted an increased rate of collisions for cars exceeding the mean travel speed. This implies that the faster a vehicle travels, the more likely it is to be involved in a collision. It stands to reason that a vehicle will come into closer proximity to more cars if it is not travelling with the flow of traffic, the amount of time available for the driver to react to an emergency situation is decreased at higher speeds, the vehicle will be more difficult to control, and the distance required to stop increases dramatically. This last point is one that is often overlooked, or is at least not perceived, by the driving public. The stopping distance is related to the energy that the brakes are required to absorb, and kinetic (and impact) energy has a squared relationship to velocity. At 60 km/h an increase of only 25 km/h results in a doubling of the energy (*see* Figure 3).

Figure 3
Don't Fool Yourself — Speed Kills!



This increase in energy must be dissipated by either the brakes or the body of the vehicle and its passengers in the event of a collision. However, individuals' perceptions of speed tend to be more linear so they do not recognise its potential danger. Whether the public are cognisant of it or not, the fact remains—the faster you go, the harder you hit, the more damage you do. This is the message that the Victorian Traffic Camera Office has been trying to get across to the community.

However, convincing people of the danger of speeding is not an easy task. Unlike drink driving, there is no social stigma attached to being a speedster. The flashy

executive or sporty youth with their racy car is a fashionable role model. And no one believes that they are a bad driver. 'I only speed when it is safe, 'everybody does it' and 'it will not happen to me' are common attitudes in the community. It is always the 'other person' who is the lunatic. It is just bad luck if 'I' happen to have an 'accident'. People cannot see that their driving behaviour is a major contributing factor to road trauma.

The problem, as seen by the Traffic Camera Office, was two-fold. Driver behaviour needed to be modified in order to reduce the level of speeding, and driver attitudes needed to change to bring about a long-term improvement in road safety. The challenge was to make speeding socially unacceptable.

The Options

Related to the three causal factors in traffic collisions—environmental, vehicular, and human—there are three basic models of attack: engineering, education and enforcement. All three had been used with varying degrees of success and had played a role in the reduction in road fatalities over the previous two decades. Examples of these models in use include campaigns for the compulsory wearing of seat belts (1970), maximum rural speed limits of 100 km/h (1973), the State Intersection Control Program (1974), random breath testing (1976), police use of radars to detect speeding drivers (1982), and the municipal bassinette loan scheme (1985). In excess of twenty government road safety initiatives have been introduced since 1970 and more were under development, yet these initiatives appeared to be just nibbling at the edges. A concentrated attack on the prime causes of collisions was required.

The engineering model

The engineering approach could address vehicle design, road worthiness, traffic management, carriageway improvement and similar issues. These are all ongoing concerns, but they only obliquely address the major cause of collisions—the driver. For large scale change, the engineering model was a prohibitively expensive option requiring medium to long-term time-frames for implementation.

The educative model

The educative approach was seen as more appropriate to the speeding issue in that it could address driver attitudes and skills, but it could not ensure a change in behaviour. For the young, external influences can often be more influential than a training regime and, for those already driving, old habits die hard. The expected time-frame for effective attitudinal change resulting from the educative model—if any change at all—was predicted to be in the order of one generation; that is, twenty to twenty-five years.

The enforcement model

Enforcement alternatives are quick to implement, costs can be contained, they focus on those most at risk (or to blame) whilst reinforcing good driver behaviour by highlighting speedsters and creating an environment for attitudinal change. Moreover, the effect of the enforcement model is immediate, releasing valuable resources for work on other areas. However, the level of enforcement must be massive if it is going to have any serious effect and must be maintained if it is to bring long-term benefits. The down side of this model is the potential for a backlash from the community when individuals are confronted with the consequences of their behaviour; especially if their belief structure tells them that they were not really doing anything dangerous. This was seen as one of the major risk factors of the enforcement model and needed to be handled sensitively for a program of the proposed nature to succeed.

Ultimately, a massive increase in the likelihood of detection was required, to be accompanied by a high level advertising/public education campaign to inform drivers of the risks of speeding and the high probability of being caught if they speed. This required the use of a new generation of speed cameras and new advertisements throughout Victoria.

The Traffic Camera Initiative

In July 1989 it was proposed that the road trauma problem be tackled by significantly increasing traffic offence detection through the expanded use of speed and red light cameras. This was to add to the five-year Victorian Speed Management Strategy (commenced in 1987) to rationalise speed zoning and encourage behavioural change in Victorian drivers. The object of the proposal was to change driver behaviour to reduce overall speed in the community, resulting in a reduction in the number and severity of traffic collisions in general, and collisions at intersections in particular. This objective was to be achieved through:

- public education; the development and presentation of a major media campaign on speeding and its effects on the road toll;
- increased speed and red light enforcement activities through the purchase and deployment of an additional twenty red light and sixty speed cameras; and
- the installation of new technology to process the images and issue the resultant penalty notices (Traffic Infringement Notices or TINs).

The public education point recognises the fact that, in our society, we police by consent. The public must be supportive of a campaign for it to succeed. The regulation of travelling speeds balances precariously between the limits on mobility and safety. The community balances the results in the posted speed limits but then individuals make their own choice and, because individuals believe themselves to be safe drivers, they believe they can go faster. Convincing these drivers otherwise was recognised as a critical success factor from the outset and extremely important in the management of the potential backlash of the Traffic Camera Enforcement Program.

The installation of new technology indicates the level of activity believed to be required to run an effective campaign. The proposed technology represents a capacity to:

- examine up to 200,000 records of evidence introduced in one month should the level of offences detected so require;
- inquire on vehicle registrations and driver licences;
- produce and issue the initial and any subsequent TINs (many nominate another driver requiring the issue of a second ticket); and
- the collection of payments, not to mention the miscellaneous inquiries and correspondence that need to be entered into.

As such the enforcement capability became the critical success factor for an effect on driver behaviour.

It was postulated that the prevalence of speeding in the community ($\mathbf{N_S}$), which is estimated by the rate of speeding offences detected ($\mathbf{R_D = N_D/N_{checked}}$) times the total number of drivers ($\mathbf{N_T}$), would be inversely related to the perception of the chances of being caught, and that this in itself was related to the level of detection achievable. That is:

$$\mathbf{N_S} \propto \frac{\mathbf{1}}{\mathbf{N_D\, e^{-kN_T/N_D}\, dt}}$$

if detection is held at a constant level.

Where $\mathbf{e^{-kN_T/N_D} = e^{-ktN_T/\ N_D dt}}$ represents a relapse response variable incorporating the effect of behavioural reinforcement $\mathbf{N_T/\ N_D dt}$.

Thus good driver behaviour would be directly proportional to the rate of detection N_D/t which is solely a function of the number of cameras available, the amount of their use, and the ability of the system to issue TINs. Moreover, the higher the level of detection, the longer the relapse time for bad habits to reform. This is crucial if long-term attitudinal change is to be achieved. It also suggests that, although resources may need to be ramped up initially to maintain the detection rate, after a period of time the effect will, to a large extent, sustain itself and require minimal future input to maintain the impact.

However, speed and red light cameras were only two of the ten key elements in the 1989 Road Safety Strategy. The overall strategy encompassed:

- a graduated licensing system;
- upgraded road safety education programs;
- thirteen new 'booze buses';
- increased random breath testing to more than 1 million a year;
- a comprehensive review of speed zones;
- repeater speed zone signs;
- sixty new automatic speed cameras;
- twenty additional red light cameras;
- compulsory bike helmets; and
- a new demerits system (Minister for Transport and Minister for Police and Emergency Services, 29 September 1989, joint press release).

The Challenge of the Traffic Camera Enforcement Program

A clear set of Traffic Camera Enforcement Program management objectives were established. These were:

- to establish a base for an overall change in driver behaviour with a 10–15 km/h general speed reduction in six to twelve months;
- as a result produce a 10 per cent reduction in collisions;
- to bring into operation sixty new speed cameras and twenty additional red light cameras and train staff in their use;
- build an automatic Traffic Infringement Management System capable of assessing 200,000 records of evidence (images) per month and have it operational within six months.

Prior to the commencement of the Traffic Camera Enforcement Program, each speed camera required four officers; two to attend the camera and two down the road to intercept excessive speeders (vehicles travelling at more than 30 km/h over the posted limit). The assessment of the film evidence using slides in a darkroom environment was also resource intensive requiring three operators for up to ten minutes per frame. The Program productivity objectives were simple:

- establish processes to enable single member camera operations; and

- build a system to enable assessment of evidence (images) at the rate of one frame per minute by a single verification operator in a standard office environment.

Given the number of vehicles exceeding the speed limit and the capacity of the cameras to take one photograph per second, it was essential to establish highly productive systems to ensure a balance between enforcement and follow up processing. The benefits of this were expected to be:

- a reduction in collisions;
- fewer deaths and less severe injuries;
- reduced compensation claims; and
- reduced hospital costs (incorporating fewer bed days and less complex treatment).

These represent significant savings to the community and form a yardstick by which the success of the Traffic Camera Enforcement Program can be measured.

The Management Miracle

The Traffic Camera Enforcement Program started at this point from ground zero, and it is no mere fluke that it has been able to meet all of its major objectives. The Program has been finely orchestrated from the outset. It has also used some significantly different approaches for a technology development program, and ones that could well be emulated to good effect on other government programs.

Coordination

From the outset Likert's theory of management linkage (Likert 1967, pp. 156–65) was deliberately adopted to maintain coordination of the Road Safety Strategy as a whole. A Ministerial Committee on Road Safety (which included both the Minister for Police and Emergency Services and the Minister for Transport was established), and a Senior Officers Joint Consultative Group (comprising officers from the Ministry for Police and Emergency Services, Roads Corporation, Victoria Police, and the Transport Accident Commission chaired by the Director of the Traffic Camera Office) was put in place to manage the major system interfaces. Thus, coordination was ensured from the outset between the government policy level, through strategic planning and support in all relevant agencies, down to the establishment and operational management of the new Traffic Camera Enforcement Program (*see* Figure 4).

Figure 4

Traffic Camera Initiative, Organisational Framework

Ministerial Committee on Road Safety

Minister for Police and Emergency Services

Minister for Transport

Senior Officers Joint Consultative Group

- Police and Emergency Services
- Roads Corporation
- Victoria Police
- Transport Accident Commission

Traffic Camera Office

Fire in the belly

A multidisciplinary team of six persons was set up to take on the task of setting up the Traffic Camera Enforcement Program. Apart from strong technical and management expertise in a range of areas, the main selection criteria for the Project Team members seem to have been initiative and inventiveness, as the philosophy for the Traffic Camera Enforcement Program was 'if it cannot be done, we will do it'.

The small team approach to development did mean that each Project Team member knew what other team members were doing. With no additional support, team members had to rely on each other for expertise. Most importantly, authority was delegated to individual team members to make decisions and act. If something needed to be done, it was; the niceties of protocol were worked out later. This often meant pre-empting changes at a higher level.

The Traffic Camera Enforcement Program was also given a limited but reasonable budget with which to work. The budget could be flexibly allocated and team members were aware of what they could commit to undertake. This prevented delays and made negotiations manageable. Strong belief in shared objectives won out against the odds—someone has got to have the fire in their belly.

Do it now

Aggressive timelines were set and met. Expressions of interest for the development of the Traffic Infringement Management System (TIMS©) were sought and shortlisted, specifications written, and requests for tender issued within two months of the decision to proceed. Tenders were received in the first week of December 1989. The responses were evaluated, contract negotiations entered into and concluded, and the contracts signed, all by 22 December 1989. This would have to be a record for a government contract of this size—particularly in the information technology area—and it required considerable ingenuity to get through the contract approval process. During the early development phase, Project Team members undertook to respond to questions regarding the specifications within one day in order to prevent delays for the developers. With no excuses for delay, the first release of TIMS© went live on 10 June 1990, only five-and-a-half months after the signing of the contract.

Stick to the knitting

The Project Team used professional contract managers from the Communications Group of the Ministry for Housing and Construction to manage the major contractual processes throughout the life of the Traffic Camera Enforcement Program. This ensured that these aspects would be completed properly and expeditiously by experts, leaving team members to concentrate on design and implementation issues rather than paperwork.

In fact, outsourcing has been a feature throughout the entire Program. Project Team members very much 'stuck to the knitting'. The Project Team did only what it was good at and acquired expert input on contract as required. The Team kept control of the design of processes and systems, management of the Office's operations, and directing developments. The Project Team's job was to build a system and set up the Traffic Camera Office.

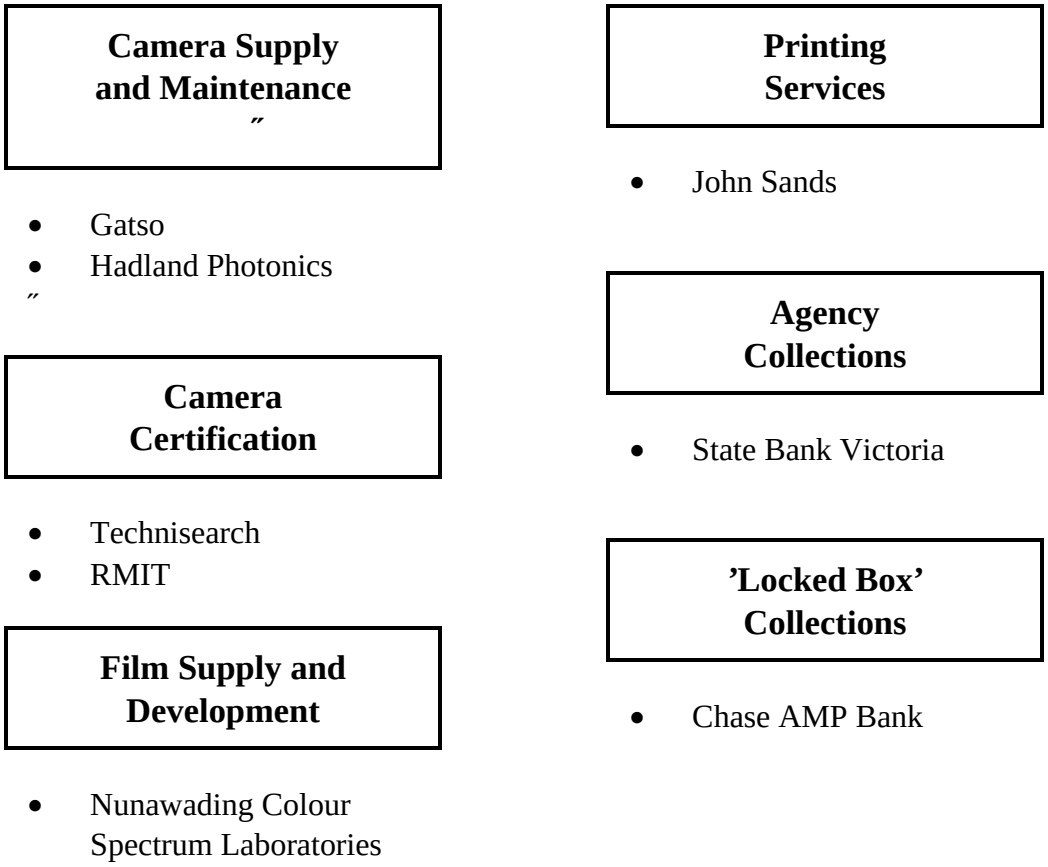
The Traffic Camera Office's (TCO) job is to process traffic infringements. It is not to develop film, nor to print stationery, nor to run banking facilities—although these are all essential components of the Traffic Camera Enforcement Program. The TCO uses sixteen private companies in its day to day work. Nearly all of these operations could have been done in-house if required, but why bother? You do not have to do a task yourself for it to be done properly as long as you control the process. All of the contracted organisations are specialists in their field; they can do it better and with fewer overheads (*see* Figure 5).

Dependent, independent, interdependent

Letting go in this manner does require a certain maturity and confidence in the management approach. Unlike a child who starts out life dependent on others, or a teenager who demands independence, a mature organisation recognises interdependencies and uses them to benefit all. This means that, rather than managing the process, the interfaces are managed.

Figure 5

Traffic Camera Initiative, External Services Contractors



The TCO quickly learnt to do this well. In processing infringements, the TIMS© system interacts with twenty-six external agents. The key to management of complexity at this level is engineering the interdependence of shared goals and the willingness to make reciprocal arrangements, even if these arrangements are not of immediate personal benefit. However, sensitive monitoring and feedback loops that provide information on external processes are still needed to ensure that everything is going as planned. These were designed and built into the processes at the outset. Interdependence was built in at the systems level to reflect the organisational design.

Creating the future

In respect of the tender for TIMS©, both it and the original request for tender were written for outcomes and results, not for equipment or technology types —as was said to tenderers *we will buy a bit of string if it will work*. Most organisations look at what is available, decide what they want and buy it. They then go to tender to get the best price. The Project Team did not. There are four ways to approach systems development:

- translate what is currently being done onto equipment that is already available. This is safe and takes a project nowhere, but hardware suppliers love it—it can be called 'mechanisation' of the past;

- look at what is required and investigate the possible techniques and design systems which may deliver the project's goals—'modernisation' of the present;

- look at what is under development and take advantage of future technological options—'designing' for the future; and

- go bravely where no man has gone before and say what it is you really want to do. Lead suppliers to skew or bring forward their development plans to achieve this—'creating' the future.

Government contracts are big enough to do the latter; the military has been doing it for years. For decades there has been two markets in technology products: defence and others. Increasingly, there is more market segmentation for high technology equipment (big or small); that is, defence, law enforcement, medical, and other users. It is time the law enforcement community used its bargaining strength to get what it requires and not just accept what is being offered by vendors. The TCO looked at the options and decided on a mixture of 'creating and designing the future'. There was no time for a full research and development effort, but the TCO went to the cutting edge of technological development, looked over and said 'that's where we want to go'. The TIMS© system is unique, superbly productive, and is poised to pick up the next wave of technology as it becomes available.

Focus the delivery

The trick to successful development is getting the right prime contractor married to the best subcontractors under a fixed price contract. Be willing to bear some of the risks—and there certainly are risks associated with this approach—but under this type of arrangement the ultimate risk of system delivery and performance resides with the contractor.

As a rule of thumb, one contract is enough. Holding multiple contracts to deliver a system can become a contractual and management nightmare. It is more expedient, and certainly more effective to only have to deal with one organisation in order to resolve issues.

Do it once, well

The TIMS© system and the operation of the TCO has been designed with one guiding principle: client service is paramount. Everything must be efficient and easy to use and items should only ever have to be dealt with once by the TCO or the client. Machines, therefore, do most of the work automatically. In fact, the greatest danger would be for things to happen without the knowledge of the right people, so the system rules and office procedure must be crafted very carefully. These concepts seem to have been quite foreign to the people for whom the system has been built. Police officers are more used to taking action than not and are not at all comfortable with their perceived lack of control in the system. Yet, every transaction is recorded and every decision is auditable. It is not easy to look at 600,000 infringements individually

and ensure that all the right actions have taken place. Therefore, educating the users of TIMS© about the processes involved is vitally important, and sometimes difficult, for if the system has been designed for efficiency it often brings into question past practices or makes redundant procedures which were previously considered essential.

Invite attention

Lastly, the TCO has been abuzz with auditors and evaluaters looking at the Traffic Camera Enforcement Program and the operations of the office in minute detail—mostly at the TCO's request. A public campaign of this type must expect scrutiny, so why not invite it. Many positive suggestions have arisen as a result of these investigations and the TCO has made good use of them. There is no better way than to find and overcome weaknesses early. The auditors and evaluaters are experts in their field, so their advice is a valuable asset to any program. As a result, the TCO has had one of the very rare positive reports issued from the Auditor General's Office; but then again, how could they complain? The TCO used audit expertise for guidance in the building of the system!

The TCO has maintained a commitment to evaluation by inviting the Monash University Accident Research Centre (MUARC) to undertake an independent, in-depth evaluation of the effects of the Traffic Camera Enforcement Program. Their report is presently in preparation.

The Proof of the Pudding — What Did All This Effort Achieve?

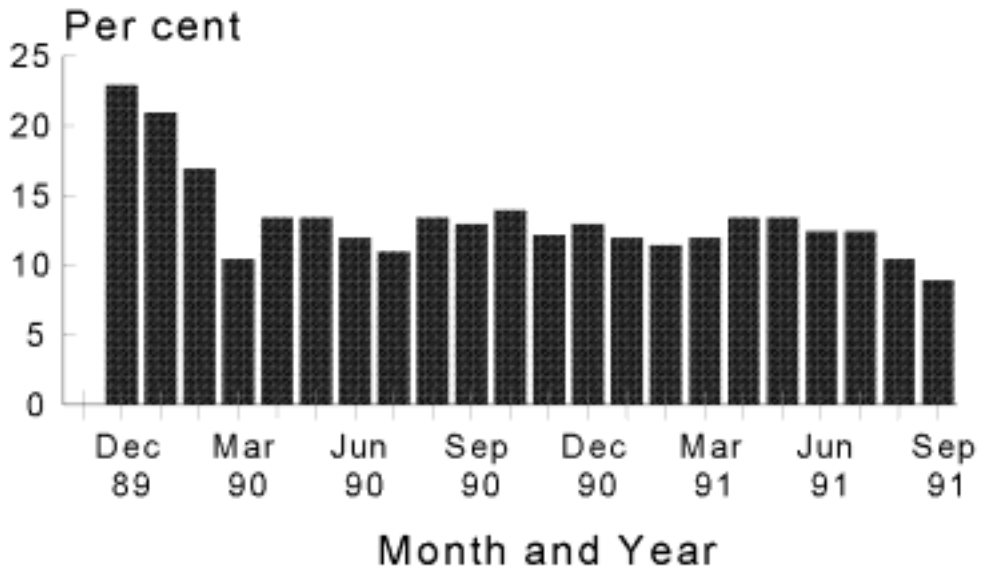
Traffic Camera Office

- Sixty speed cameras progressively introduced from December 1989 (four units) to August 1990; single officer operations commenced in August.
- The TCO was established from a zero base, firstly to a project team of six in December 1989, then to a staff of thirty in February 1990, to its final complement of 100 by December 1990.
- Implementation of a $23 million road safety program.
- The TCO commenced automated processing on TIMS© on 10 June 1990—just five-and-a-half months after signing the development contract (22 December 1989) with the assessment of images at the rate of two per minute (twice the target rate).
- Government Technology Productivity Award presented for TIMS© at the Government Technology Event in February 1991.

Deterrent effect on speeding

- Camera operations resulted in 8.2 million vehicle speed checks during 1990–91. Over 20,000 speed checks per day, which has risen to more than 50,000 during the first four months of 1991–92.
- This increased enforcement, combined with the shock advertising, has led to a sharp reduction in the percentage of vehicles being photographed; from 23 per cent in December 1989 down to 11 per cent in June 1990, and a further reduction to 8 per cent in October 1991 (*see* Figure 6).

Figure 6
Vehicle Speeds
Vehicles Travelling Above Threshold



- 374,050 TINs issued during 1990–91 with a further 280,000 issued from July to October 1991.
- The proportion of excessive speed offences (30 km/h or more over the limit) has also fallen sharply from 1.6 per cent in December 1989 to 0.6 per cent in June 1990 and 0.5 per cent in September 1991 (*see* Figure 7).
- The number of vehicles speeding through the VicRoads speed monitoring sites has fallen sharply since the Traffic Camera Enforcement Program began across all speed zones, but particularly in the 100 km/h areas (*see* Figures 8, 9, 10).

Figure 7
Vehicle Speeds
Per cent of Vehicles Travelling 30 km/h or More Above Limit

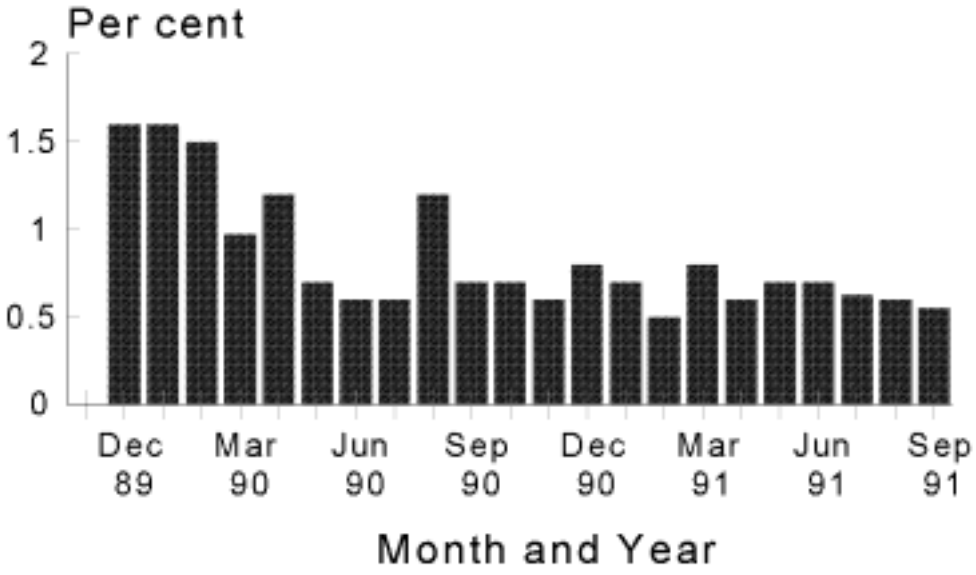


Figure 8
Speed Monitoring Project
Per cent of Vehicles Exceeding Speed Limit
60 km/h Speed Zones

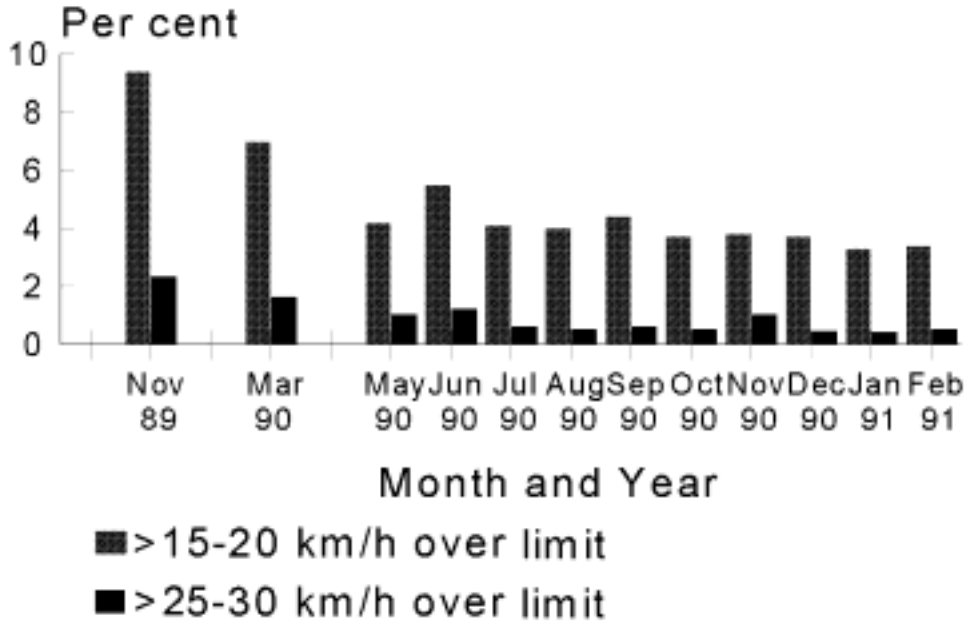


Figure 9
Speed Monitoring Project
Percent of Vehicles Exceeding Speed Linmit
75 km/h Speed Zones

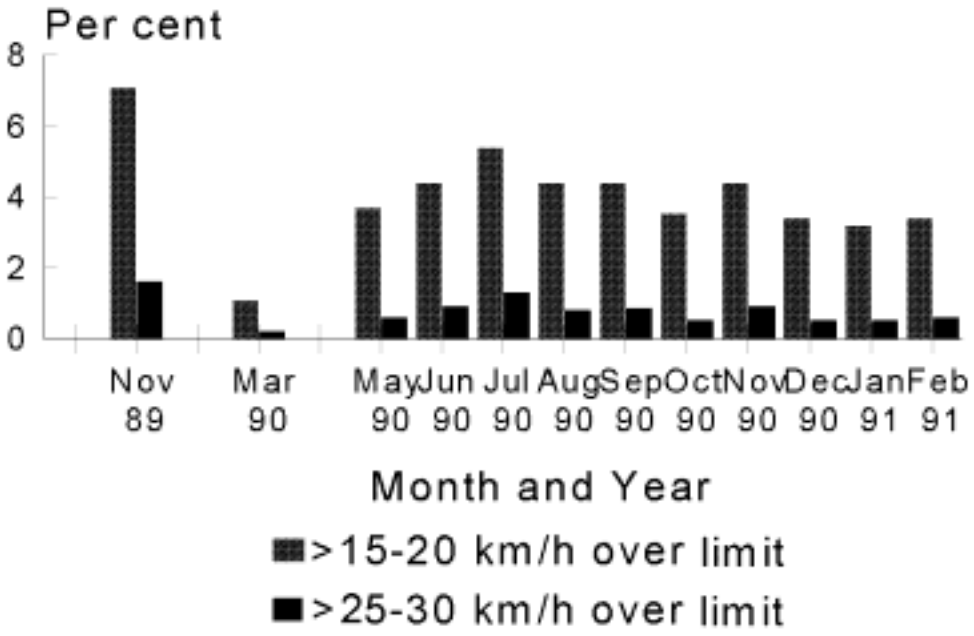
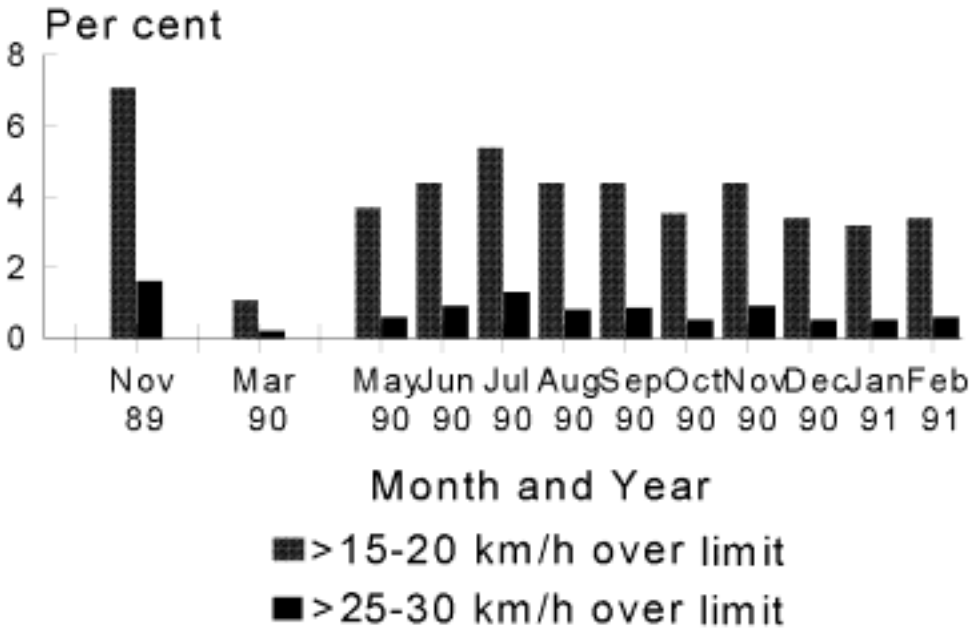


Figure 10
Speed Monitoring Project
Per cent of Vehicles Exceeding Speed Limit
100 km/h Speed Zones



Road safety outcomes

- Vehicle collisions fell 16 per cent in 1990, and a further 9 per cent to August 1991 (*see* Figure 11).

- Contributed to the 30 per cent reduction in fatalities in 1990—229 lives saved. A further 21 per cent reduction was recorded during the first half of 1991 (*see* Figure 12).

- In 1990, injuries resulting from traffic collisions fell by 21 per cent including a 22 per cent drop in injuries requiring hospital admission, a saving of over 8,000 bed days made available for other urgent treatment (*see* Figure 13).

- The reduction in road traffic collisions, fatalities and injuries during 1990 saved Victorians over $300 million in hospital, compensation, lost productivity and property damage costs.

Figure 11
Collisions, Victoria January 1987–December 1992
(moving twelve-month total)

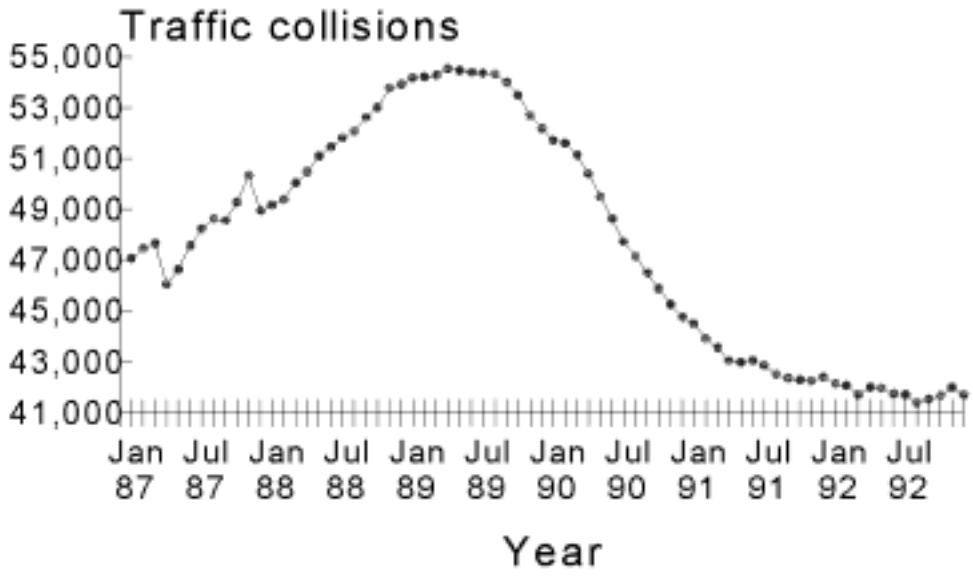
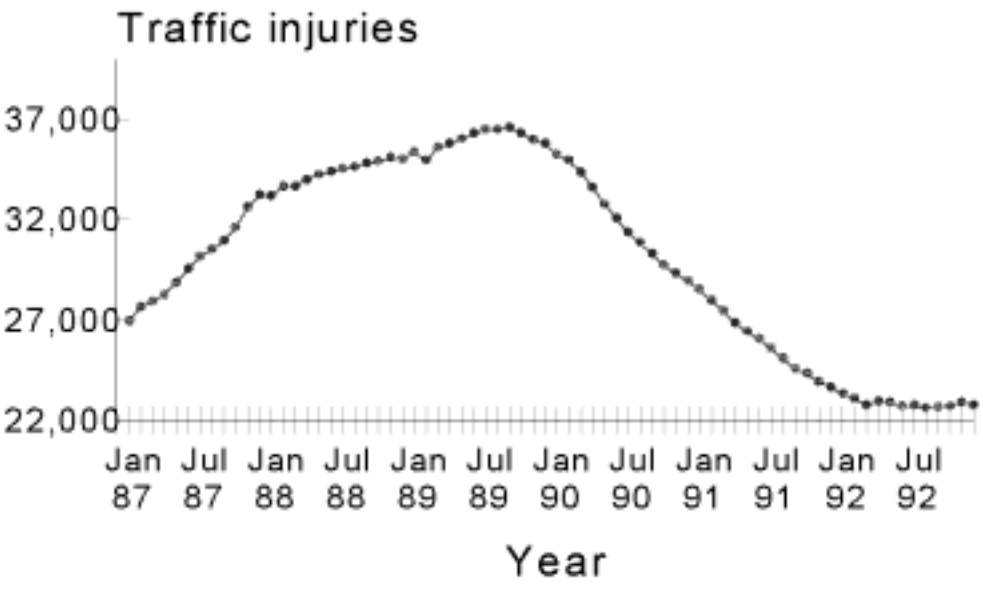


Figure 12
Fatalities, Victoria January 1987–December 1992
(moving twelve-month total)

Figure 13
Injuries, Victoria January 1987–December 1992
(moving twelve-month total)



It is interesting to note that the TCO's original estimates for the reduction in the number of collisions has since been shown to be conservative, although it was not thought to be at the time. Recent European research suggests that the change in the rate of collisions is in the order of a fourth power relationship to the general reduction in velocity (Gerondeau 1991) rather than the squared relationship that had been assumed, so massive collision and road toll reductions are now predicted from relatively small behavioural shifts. The Victorian experience supports these findings.

On this basis the TCO can confidently predict further significant gains given a sufficiently high level of enforcement to maintain the lower speeds on our roads.

Something Has Changed

The motoring community has clearly reacted to the perceived risk of being caught speeding. This perception has been raised many fold by:

- high impact of advertisements;
- the knowledge that speed cameras are deployed throughout Victoria —one could be around the next corner;
- discussion in the community, especially with people who have received a ticket;
- actually receiving a ticket—or even more than one.

Three areas of community concern are continually raised. The first is that speed limits are not well-posted or are too low. Over 20,000 repeater speed signs were installed before the introduction of the cameras in 1989, and all speed zones, especially the intermediate zones (those between 70 and 90 km/h) have been reviewed before enforcement. In addition, the location of camera sites is related to the collision and road toll history for the area and needs to be sensitive to the reasons for the local speed zone; for example, the time of day or year for shopping or school activities and special events.

The second issue poses the question: *why are police chasing drivers and not other criminals?* Of course, exceeding speed limits is against the law and the fact is that injuries are more severe in higher speed collisions. The police resource requirement for the Traffic Camera Enforcement Program is very low compared with the massive road toll savings, and police time is freed in having to attend fewer collisions.

The third issue often raised is that traffic camera enforcement has been increased simply to raise additional revenue. It is a fact in all law enforcement jurisdictions that monetary penalties are applied to a very wide range of offences, including traffic offences, as a first option to avoid the more punitive licence loss or expensive custodial options. Moreover, the road safety benefits in terms of reduced road trauma and decreased demand for health care services far exceed the value of revenue collections. In addition, all motorists enjoy the benefits of safer road use which is reflected in reduced vehicle insurance premiums.

Even given these concerns, 80 per cent of respondents in a recent survey support the use of speed cameras because they 'slow drivers down', 'reduce collisions', and 'catch speeders'.

Future Directions

The paths are many and varied but the TCO believe the next few years will see installations along the following lines.

Video imaging

Traffic camera images can be captured and processed at remote sites with the image and offence file transported or transmitted to the central processing bureau, in our case, the TCO. The challenge here is to balance resolution and data file size with broad enough band width to enable real time communications. This would enable on-line infringement processing without the delay inherent in film processing; perhaps even same day 'service'.

Remote data entry

Equipment is already available to allow 'on the spot' penalty notices to be issued using a hand-held device with in-built data memory, which is downloaded to a central processor at the end of a shift. This provides automatic remote data capture which overcomes the mistakes inherent in duplicating data entry, particularly when using a field produced handwritten copy as the data entry form.

Remote data inquiry

Again the equipment is already available—and being used in South Australia and many other jurisdictions—to give officers at the sharp end (on the street) on-line inquiry access to vehicle, driver, and offence databases. This allows the officer the benefit of reviewing relevant information prior to or whilst interviewing a driver in the street. Given suitable image compression techniques, this could be extended to high quality digital images in vehicles, police stations, and maybe even on the beat.

Document imaging

This is a fast growing field and one that could be well-used in the police environment given the plethora of forms and official documents in daily use. Hierarchical processes of their nature have documents handled sequentially with time delays between each step. Office automation networks encompassing the scanning and storage of externally produced documents facilitates efficient and effective records management and a speedy decision process.

Shape and pattern recognition

The TCO image handling software, which is designed in part to find and recognise a defined shape in 2D space, has wide applications outside traffic enforcement. The ability to identify vehicles without the use of an expensive transponder grid infrastructure allows a number of new roadside applications; for example, road pricing on roads, bridges or tunnels either by prepayment with recognition of the on-vehicle receipt or sticker, or periodically billing against the vehicle registration plate if the prepaid sticker is not found. The same applies to pricing for car parking spaces, whether at the side of the road or in a private parking station. These principles can apply to the recognition of any alphanumeric patterns, for example, identification tags

on cargo or containers, on aeroplanes as they enter or leave airport facilities, or production line goods.

Combined with a remote image capture system and vehicle registration identification process, a roadside system for the analysis of exhaust gases—and thus the identification of polluting vehicles—would allow these vehicles to be referred for further testing and maintenance.

Fiasco

Automated fingerprint comparison systems now provide a powerful investigative tool for police. The recent upgrading of the identikit process using computer-based imaging techniques to build a facial likeness has significantly improved the quality of identikit photos provided to the public. Why not combine the concepts?

Identikit provides a picture, but of whom? A combined Facial Image Analysis System and Comparison Operation can be envisaged which would analyse facial characteristics, search a database and use the results to answer this question in a similar manner to the NAFIS system for fingerprints.

These systems are not pipe dreams; they are all realisable now. It only takes the political will to create them. Victoria, through the Traffic Camera Office, now leads the world in the application of high technology for traffic law enforcement. The results speak for themselves. With a little initiative and some creative information technology management, similar benefits could be reaped across a wide spectrum of policing activities.

References

Australia. Bureau of Transport and Communications Economics 1989, *Social Cost of Transport Accidents — Australia*, Australian Government Publishing Service, Canberra.

Fildes, B.N., Rumbold, G. & Leening, A. 1991, *Speed Behaviour and Drivers' Attitude to Speeding*, Report No. 16, Monash University Accident Research Centre, Clayton, Victoria.

Gerondeau, C. 1991, 'Report of the European Communities Commission Expert Group on Road Safety', Association for the Promotion of Road Safety Techniques, Paris, France.

Likert, R. 1967, *The Human Organisation*, McGraw Hill, New York.

Munden, J.W. 1967, 'The Relation Between A Driver's Speed and His Accident Rate', Laboratory Report 88, Road Research Laboratory, Crowthorne, UK.

Research Triangle Institutes 1970, 'Speed and Accidents', Highway Safety Bureau, Durham NC.

Solomon, D. 1964, *Accidents on Main Rural Highways Related to Speed, Driver and Vehicle*, US Department of Transportation, Federal Highway Administration, Washington DC.

VicRoads 1991, 'Accident Statistics 1990', VicRoads, Melbourne.

VicRoads 1991, 'Road Accident Facts 1990', VicRoads, Melbourne.

VicRoads 1991, 'Road Safety: Challenges and Strategies for the Next Decade', VicRoads, Melbourne.

VicRoads 1991, 'Attitudes to Speed—Wave Four', Report 1, Summary of Results, VicRoads, Melbourne.

Victoria Police. Traffic Operations and Support Department, Policy and Education Division (various years), *Road Traffic Collisions Analysis: monthly report*, Traffic Operations and Support Department, Melbourne.

TRAFFIC POLICING: RED LIGHT/SPEED CAMERAS

Wayne Jones
and
Bruce Leggatt
Image Applications
New South Wales

IMAGE APPLICATIONS, AN AUSTRALIAN COMPANY SPECIALISING IN IMAGE capturing and computer programming, has been supplying processing equipment for red light cameras to police since 1988.

The red light camera processing system involves a device that allows for the manipulation and enlargement of silver halide film and the conversion of the images to a composite video signal. In that format, the images can be viewed on monitors or digitised into a computer database.

At the instigation of a number of police forces in Australia and overseas, Image Applications have taken their expertise a significant stage further. Their new automated traffic camera system, Image Master©, was unveiled at the Asia Pacific Police Technology Conference in 1991.

In developing the Image Master system, Image Applications set out to satisfy the optimum criteria guidelines set by the various police forces. The system, to be totally cost-effective, needed to meet the following requirements:

- dramatically improve the capture rate of red light offences in any one of one, two or three lane installations;
- achieve acceptable capture rates in four lane installations, which existing technology could not achieve;
- operate effectively regardless of light conditions (including variations from morning sunlight shining directly onto the lens to afternoon sun casting shadows across the number plates); and
- improve the quality of night time images by overcoming the problems associated with flash lighting.

According to Bruce Leggatt of Image Applications, until 1991, the weak link in the traffic camera concept has always been the original image quality. This fact led Image Applications, in conjunction with research and development colleagues in Japan, to turn their attention to the camera. They were guided by the need for police to be able to provide image integrity to the courts, enabling images to be presented as admissible evidence; that is, the images must be untampered with.

The New System

With the Image Master system, the camera not only acts as a red light camera; it can also record speed through an intersection, speed offences on the open road and can be an attachment to existing radar and laser guns.

In meeting the criteria set out above, the Image Master system now offers police a total integrated system with more potential applications in automotive use than any existing technology. Because of the 'one camera for all jobs' approach, maintenance savings of up to 75 per cent are possible when compared with using a number of different, non-compatible systems. The Image Master system is highly versatile, extremely flexible, and can:

- automatically change its focal length from 35 mm to 70 mm, depending on the lane in which the offence occurred;
- pre-program its flash according to the light conditions and the traffic lane which triggered the camera;
- automatically change angles from 0 degrees to 30 degrees to obtain best possible image from all lanes;
- measure speeding vehicles through an intersection;
- be used in *existing* red light installations;
- be used with *existing* radar and laser operations;
- be programmed to accept or reject any number of borderline offences, in any mode of operation; and
- be compatible with any of the existing technology and systems.

To provide these diverse and somewhat spectacular features, the camera used in the Image Master system has more computing technology than many personal computers; that is, it has the computing power necessary to make the camera do exactly what is wanted. This sophisticated technology has made the system easier to use. The simplicity of the Image Master system enables an operator to install the camera at an existing location in a matter of minutes. All an operator need do is place the camera in the box, connect the plugs for the pick-up loops and power, plug in the data card which holds the programs for that intersection, attach the film magazine, enter their operator number and wait a few moments for the camera to complete its automatic self-check. A more experienced operator can actually reprogram the system on site.

Image Master cameras contain a data card. Similar to a 'black box', the data card records every action made by the camera. When removed and plugged into a computer, the data card transmits this information without the need for re-keying it. If required, the data card can record every activity that happens at that intersection, not only within the camera, but total traffic statistics.

When used with Image Master adjudications equipment and programs, this level of integration not only provides more comprehensive data but frees the adjudicating operator from a mundane task, leaving more of the operator's time and concentration to the important decision: does the image being viewed constitute a prosecutable offence?

While each Image Master system can perform all of the functions outlined in this paper, no two systems are the same. Image Applications works on a needs basis; that is, aiming to satisfy the needs of the particular police force installing the system. Rather than one package being made available to all, the Image Master system is tailored to the individual police force.

MOBILE SATELLITE COMMUNICATIONS

Greg Ellis
OPTUS Communications Pty Limited
Sydney
New South Wales

THIS PAPER WILL DESCRIBE THE SERVICES OFFERED BY **mobilesat**™ AND how these services may be used to solve the problems experienced by many organisations when trying to communicate their remote field personnel.

A key requirement of communication networks (especially emergency services) is the ability to reach anybody, anywhere, anytime. By their very nature, existing ground-based mobile communications networks are limited by the Australian environment, resulting in blind spots, intermittent connections and garbled transmissions which, in the extreme, could potentially compromise user safety. Associated with these problems is the cost of expanding the terrestrial base station infrastructure in an attempt to widen coverage and the cost of then maintaining these widely-dispersed bases.

OPTUS will be providing a range of mobile satellite services, namely **mobilesat**™, throughout Australia in 1993. These services will include circuit-switched voice/data services and data messaging services for land, air and marine applications. This will make Australia the first nation in the world to provide the complete range of land mobile voice and data satellite services.

The **mobilesat**™ system is categorised into three services: public, private and thin route data which will utilise L-Band capacity on the second generation spacecraft, the first of which was launched in 1992. These services will be created from four generic features:

- voice;
- data;
- facsimile; and
- packet switched messaging.

Voice

The **mobilesat**™ voice feature offers full duplex connection into either the public switched telephone network or within a defined closed user group of a private network. The voice quality is extremely high, even under severely shadowed conditions, due to the voice codec selected for **mobilesat**™, which was developed by the Massachusetts Institute of Technology and Digital Voice System Inc. of the USA. This codec will be used internationally in similar networks. The communication channel rate will be 6.6 kbps.

Data

The **mobilesat**™ data feature will allow a laptop, personal computer or application-dependant terminal to access another terminal or host computer for bi-directional information transfer. Possible police applications would be licence/registration checks, incident dispatch or reports filed direct from the field. The transmission rate will be 2400 BPS asynchronous and it is protected by forward error correction.

Facsimile

The **mobilesat**™ circuit switched facsimile feature will provide an end to end connection for group facsimile and will operate up to 4800 BPS.

Packet Switched Messaging

The packet switched messaging feature provides for the transmission of short messages between a **mobilesat**™ terminal and a user dispatch centre, using reserve capacity on the signalling channels. This feature is designed for the transmission of global position system data (GPS) or status type messages.

Services

Public access service

The public access services will be mobile telephone service with direct access to the Public Switched Telephone Network (PSTN). Access to the PSTN will be via an OPTUS gateway. Call charges will be distance independent. **mobilesat**™ is designed to offer Integrated Services Digital Network (ISDN) type features such as caller-ID.

Private network service

The **mobilesat**™ private network service is designed for organisations who have a fleet of field vehicles or remote area stationary applications and require mainly internal communications. The operation of a private network will be based on the concept of closed user groups and will offer the following call types:

- a private call from **mobilesat**™ terminal to base, base to terminal or terminal to terminal call;
- a broadcast call where all user group members will hear the calling party; and
- a group call where all group members are able to participate in the conversation.

Additional private network features include:

- interconnects with an existing UHF/VHF terrestrial network;
- interconnects with the user's private automotive branch exchange (PABX); and
- emergency priority channel access, where the user activates the emergency button on the terminal.

A **mobilesat**™ private network will give the user two types of design options:

- a *shared base* station where the user accesses their network via a land line or microwave connection to an OPTUS earth station in Sydney or Perth; or
- a *minor base* station located on the user's premises.

The third service is thin route data which will use packet switched messaging for the transfer of small amounts of data; that is, telemetry and Supervisor Control and Data Acquisition (SCADA) or alarm monitoring.

Reliability

The reliability of the **mobilesat**™ system is assured. The system is designed to initially support up to 1,000 circuits. Key sub-systems are fully redundant. The sophisticated digital signalling and coding techniques employed guarantee resistance to shadowing and multipath fading. 'L' Band transmissions are not affected by rain, atmospheric conditions or sun spots. In addition, each **mobilesat**™ terminal is capable of becoming the controller, offering the ability for a site command to control all or part of a network.

Security is another important area in police communications. The voice feature is based on the latest low bit rate digital voice codec and this, in conjunction with the random allocation of channels, means that casual eavesdropping will be virtually impossible. Similarly, the facsimile and data features are protected in this manner. For very secure communications, an encryption device should be fitted to the **mobilesat**™ terminal or facsimile/data interface unit.

Conclusion

With the introduction of the **mobilesat**™ services in 1993, high quality, flexible and reliable communications will be available to everyone in Australia regardless of their location. No longer will police personnel be required to operate in areas isolated from the communications that are essential for them to perform their duties efficiently and with safety.

DRUGS — THE ROLE OF THE AUSTRALIAN BUREAU OF CRIMINAL INTELLIGENCE AND THE AUSTRALIAN CRIMINAL INTELLIGENCE DATABASE

Keith Askew
Assistant Commissioner
Director
Australian Bureau of Criminal Intelligence
Canberra
Australian Capital Territory

THIS PAPER WILL OUTLINE THE ROLE AND FUNCTIONS OF THE AUSTRALIAN Bureau of Criminal Intelligence, introduce the Australian Criminal Intelligence Database and, by doing so, explain how these resources assist law enforcement in combating illicit drug activity within Australia.

The Australian Bureau of Criminal Intelligence

In the late-1970s and early-1980s a number of Royal Commissions recommended the establishment of a national intelligence unit to combat the activities of organised criminal elements that were not restrained by state or territory boundaries, but which limited the efficiency and effectiveness of law enforcement. As a consequence of these recommendations, the Australian Bureau of Criminal Intelligence (ABCI) was established by the Australian Police Ministers' Council in 1981, following consultation and a signed agreement between the Commonwealth, all Australian states and the Northern Territory.

The role of the ABCI is to provide facilities for the collection, collation, analysis and dissemination of criminal intelligence, with a view to providing such intelligence to Australian law enforcement agencies to enable them to combat organised crime in

Australia and, in particular, to assist them to combat illicit drug trafficking. The main functions of the ABCI are:

- research and distribution of criminal intelligence;
- liaison;
- identification of national projects for operational action; and
- recommendation of proposals for legislative changes to combat organised crime.

The intelligence interests of the ABCI, in so far as they have an interstate, national or international connotation, include:

- illicit drug trafficking;
- illicit gambling;
- fraudulent dealings in shares or securities and company frauds;
- national and international movement of profits of organised crime;
- corruption in public life;
- usurious loans;
- prostitution within the area of organised crime;
- any other business interest activity with an organised crime connotation; and
- movement of persons connected with organised crime to and from Australia and their activities within and outside Australia.

The ultimate responsibility in matters of policy for the ABCI rests with the Australian Police Ministers' Council. The ABCI was established to assist and provide liaison between all Australian law enforcement agencies, and it is the expressed intention of all parties to the ABCI Agreement, that the administration and operation of the ABCI and the performance of its functions remain independent of any one participating government or agency.

In support of this policy, a Management Committee of all Australian Commissioners of Police is responsible for the direction and control of the ABCI. The Director of the ABCI is appointed to administer the Bureau, to control its operations and is responsible to the Management Committee.

When the ABCI was established, it primarily served the police forces of Australia and committed resources to those areas of organised crime that were determined, at that time, to be impacting across all police jurisdictions. Such areas included:

- cannabis cultivation and distribution;

- heroin importation and distribution;
- amphetamine manufacture and distribution; and
- cocaine importation and distribution.

Many of these commodities were imported, cultivated or distributed by specific ethnic organised crime groups at that time; for example, Italian organised criminals were responsible for the cultivation and distribution of cannabis.

Since the inception of the ABCI, law enforcement has recognised that organised crime in Australia has expanded into other, more apparent legitimate areas of lucrative criminal activity. Organised crime infiltration may now be found in control of areas as diverse as the sex, gambling, building, financial or entertainment industries. Other legitimate activities such as banking, property development and even restaurants are being manipulated by organised crime groups to provide a vehicle for the 'laundering' of the proceeds of crime.

Another emerging factor is that the serious and deteriorating economic climate prevailing in Australia has concentrated the focus of government attention across the country on matters of finance, productivity, greater accountability, managerial flexibility, creativity and innovation. Government and industry leaders alike are seeking ways to significantly enhance the international competitiveness of Australia in every area of activity.

Some of the processes used to improve Australian competitiveness are manifested in micro-economic reform initiatives including restructuring of organisations (for example, flattening), decentralisation, restructuring of industrial awards, multi-skilling arrangements, integration of disciplines and skills and similar reforms. Many of these initiatives challenge the traditional roles, methods, functions, processes, procedures and approaches of the past and many are being introduced into police forces across Australia.

Approaches of the kind mentioned previously in this paper offer the opportunity to remove impediments to efficiency and effectiveness, the thrust of which was highlighted in a speech made in 1990 by the Prime Minister, Mr Hawke, in an address to the National Press Club. He stated:

> Today we face together, challenges impossible to envisage a century ago. But the same qualities—the work, the will, the leadership—which were needed to create the Federation in the last decade of the nineteenth century are needed again . . .
>
> The goals are to improve our national efficiency and international competitiveness, and to improve the delivery and quality of services governments provide. We need to remove the impediments and the anomalies which stand in the way of those goals (Hawke 1990).

The influence of austere budget cuts by governments are having significant impact on the activities of law enforcement agencies across Australia, forcing Chief Executive Officers to do more with less.

One initiative taken by Commissioners of Police to cope with the difficult budgetary constraints within their forces has been to seek an enhanced alliance of their intelligence bureaus with the mission and objectives of their organisations and, as well, are seeking greater input from the intelligence areas within their forces on operational, tactical and strategic planning and policy development activities.

Commissioners of Police understand that this closer alliance with the mission and objectives of the organisation, along with specific initiatives to assist in operational, tactical, strategic planning and policy development, will require significant changes to the culture of traditional intelligence agencies. These changes will require a capacity to effectively cope with such issues as:

- a wider client group;
- a client group seeking a higher level of professional service;
- greater openness;
- improved levels of cooperation;
- enhanced coordination of effort;
- the integrated use of multi-disciplinary skills;
- an improved proactive approach to the use of intelligence;
- a focus on outputs;
- improved selection procedures for staff;
- enhanced training procedures; and
- a problem solving approach.

Consequently, Australia's police forces also recognised the need to liaise with other law enforcement agencies to more effectively counter this expansion of organised crime.

As a consequence of this recognition, the ABCI now not only liaises with police forces in the processing of criminal intelligence, but also with many other agencies who are also engaged in the fight against organised crime. These other agencies are diverse in nature and include national bodies such as the National Crime Authority, Customs, Immigration, Quarantine and Taxation. The ABCI also liaises with state agencies such as the Criminal Justice Commission in Queensland, and the Independent Commission Against Corruption and the Crime Commission in New South Wales.

In order to more effectively support law enforcement agencies in detecting and combating this spread of organised crime in Australia, the ABCI has developed a more flexible structuring of resources. The ABCI is now able to take a more dynamic

approach to the type of organised criminal activity it examines. This activity may range from drug trafficking, extortion and arson, to money laundering, immigration abuse and collusive tendering, by way of example. Moreover, these activities require analysis of problem areas from a much broader perspective, requiring a variety of skills from various disciplines. The ABCI, as it moves into its second decade, has evolved into an organisation better equipped to pursue and combat the enterprises of organised crime.

In undertaking assessments of organised criminal activity impacting on Australia, the ABCI adopts two styles of approach. Tactical assessments are prepared in regard to the specific criminal activities engaged in by criminal groups. These assessments identify the criminals concerned and make recommendations to the law enforcement agencies for investigative action. Strategic assessments are also prepared in relation to identified or perceived organised crime trends. This second type of assessment proposes regulatory, policy, or legislative initiatives designed to combat or prevent a recognised or developing organised crime issue.

The preparation of these assessments requires a highly manipulative, relational database, upon which the ABCI and the associated law enforcement agencies it supports can store collected intelligence data.

The Australian Criminal Intelligence Database (ACID)

The Australian Criminal Intelligence Database (ACID) is the only national criminal intelligence database in Australia. As organised crime spread into more aspects of Australian life, it became more national and international in its sphere of influence. Law enforcement, and criminal intelligence in particular, needed to develop more modern, flexible and dynamic approaches to combat it. Consequently, through ACID, Australian law enforcements' capacity to store, manipulate and retrieve intelligence has needed to develop into a more flexible and manipulative resource.

ACID evolved from the Australian Drug Database, Law Enforcement Component, and is located on the ABCI's own mainframe computer. All Australian police forces are connected to ACID by way of encrypted, high speed lines. This database holds considerable intelligence data in a manner that enables its users to perform both simple and complex searches across the stored data, establishing a comprehensive variety of linkages. It is a secure database which keeps pace with the international developments in criminal intelligence and provides a significant resource to Australia's criminal intelligence analysts for operational, tactical and strategic planning, and policy development.

This database stores intelligence data that can be manipulated so as to aid in the recognition of emerging crime trends, the identification of criminals and the criminal activity engaged in.

The manner in which this data is collated within the system will also enable the law enforcement data to be matched with data collected by the state and federal Health Departments and the Australian Bureau of Statistics. Relating this approach to illicit drugs will enable a more integrated picture of Australia's 'drug problem' to be produced, which will not only be of value to law enforcement, but to the health and educational organisations involved and the decision and policy makers.

Technology Associated with ABCI and ACID

The ABCI Management Committee and the Australian Police Ministers' Council have chosen to develop an open systems approach in the design of a computer facility for use at the ABCI in respect to ACID. This open system approach and the ACID design philosophy provides the opportunity for:

- the greatest flexibility in the inter-connectivity of disparate computer hardware operated within respective law enforcement agencies;
- the ability to select software solutions independent of hardware platforms thus avoiding being locked into any proprietary hardware or software solution;
- portability of developed software thus providing economies in the development of software applications and module design;
- lower overall establishment and operating costs;
- the development of reliable high speed encrypted communications lines to provide the link between the ABCI computer operating ACID and the law enforcement agencies, with excellent response times;
- the development of user friendly fast input screens to capture factual data and provide the automatic linking of entities giving a speedier method of input processing;
- the capacity to interrogate the data by entity, relationship (link), text, and interest. These could include individuals, organisations, commodities, type of crime, industry base, special interest groups, or any combination of these;
- the ability to browse entities through the linking mechanism enhances the usefulness of ACID as an analytical tool by providing the means to interface with third party analytical software products to display the associations graphically;
- the capacity to develop an interface with third party products for the purposes of statistical presentations;

- the use of fourth generation software development tools to produce a wide range of reports addressing the needs of the various clients.

In the future, the open systems approach provides the ABCI with the ability to:

- transfer documents or images directly into ACID with minimum operator intervention;
- develop expert systems which access ACID and retrieve data directly based upon the analyst's premise;
- utilise graphical interfaces by using windows and icon technology with mouse driven pull down assist menus or functions;
- develop additional ACID modules to deal specifically with financial transactions including financial analysis;
- provide the means whereby a database connection to other disparate state and federal databases can be executed transparently;
- develop a standard data entry methodology for use by all law enforcement agencies;
- develop a secure means for dial-in connection to remote laptop computers for intelligence related activities; and
- provide a common message switching facility for use by the intelligence community.

Conclusion

In conclusion, criminal intelligence in Australia has evolved into a process that enables law enforcement to adopt a more integrated approach to organised crime. The more flexible approach to tactical intelligence enables law enforcement to tackle the spread of organised crime with greater effectiveness. The emergence of strategic intelligence enables law enforcement to adopt a more proactive stance in relation to organised crime—to prevent some emerging problems, rather than to wait and assume a more reactive stance.

References

Hawke, R.J. 1990, Towards A Closer Partnership, speech given at the National Press Club, 19 July.

THE NATIONAL POLICE RESEARCH UNIT / TECHSEARCH / 3M AUDIT BAG

Des Berwick
Executive Officer
National Police Research Unit
Adelaide
South Australia

THIS PAPER WILL DISCUSS THE DEVELOPMENT OF A TAMPER-RESISTANT EXHIBIT bag and address the application of 'low end' but still highly effective technology to overcome a perceived problem. The solution involved some plastic, some paper and some glue, plus a lot of lateral thinking.

Genesis/Philosophy—The Drug Exhibit Project

Following a number of Royal Commission findings and media reports concerning drug exhibit handling protocols, the National Police Research Unit (NPRU) was, in 1983, instructed by its Board of Control to examine drug seizure protocols, particularly the practices, procedures and associated hardware utilised from point of seizure to point of destruction.

A senior police officer was seconded as the project's Senior Research Officer and Techsearch Incorporated, the commercial arm of the (then) South Australian Institute of Technology, was commissioned to provide technical support and input.

An examination of current Australian and overseas practices quickly made it clear that an improved exhibit container was required as a fundamental step to improved drug exhibit security.

Options Investigated—Secure Bag/Storage System

A prototype security container was developed by Techsearch in consultation with the NPRU. The container addressed the most important principle of security in terms of minimising the time between actual seizure and first accountability by means of a suitable tell-tale seal to ensure the integrity of the exhibit is maintained along with continuity of the chain of evidence.

Feasibility trials in the field under normal drug squad working conditions were carried out in mid-1984 with the South Australia Police Drug Squad, the Queensland Police and Australian Federal Police Drug Squads in Brisbane, and the Northern Territory Police Drug Enforcement Unit.

The field trials were assessed as an outstanding success not only in terms of the concept of the container, but also for the advantages of an Australia-wide uniform approach to seized drug handling procedures.

At that time, the NPRU also investigated the viability of chemical contamination of drug seizures but this was not pursued due to technical and forensic considerations identified by our technical consultants.

Description of the Audit Bag

Design considerations

The following design considerations were identified following consultation with all Australian police forces.

Identification of container: To reduce the possibility of theft with substitution, each container should be serially numbered and treated as an accountable item. It should not be possible to alter or erase this number without making the change obvious.

Chain of evidence: To preserve and simplify evidence of continuity in handling the exhibit, the container should be openable and resealable by authorised persons. There should be provision for each opening and resealing to be recorded on the container.

Availability of containers to possible users: Seizure of suspect material may be made by any police officer or agent at any time. It should therefore be readily available. The container must therefore be light and self-contained. Any sealing that requires other equipment is undesirable. The need for accountability should not limit the availability of the container.

Immediate sealing at point of seizure: The sealing method should be 'built in' and simple to use. Once closed, it must not be possible to re-open the container without detection.

Security: The material of the container should be heavy enough to be as strong as its closures. It must not be easily punctured by sharp objects inside.

Container construction

With the design considerations in mind, the *Audit Bag* was developed. The bag is constructed of clear PVC with a large pocket in the top for the storage of exhibits, labels etc and a much smaller pocket in the bottom for cross-check label storage.

The top pocket has five adhesive strips to allow for re-opening and resealing by authorised persons. Accordingly, the same bag may be used from time of seizure, through forensic and other examination to final destruction, providing both cost and chain of evidence advantages. Facing each adhesive strip is a printed security strip which bonds strongly to the adhesive.

Security features

Considerable effort and testing has gone into the construction of the five adhesive and printed strips as these provide the principal tamper-resistant capacity of the Audit Bag. Once sealed, any attempt to re-open the seal will cause visual degradation and damage to the printed strip. Such damage should be evident to the naked eye thereby providing a simple and effective visual check of exhibit integrity. As will be discussed later in this paper, considerable attention has been paid to confirming the performance of the printed strip against normal and exotic attack; for example, freezing, melting or chemically-induced adhesive breakdown.

It should be stressed that the resealability of the Audit Bag relates only to authorised opening and resealing of the bag in relation to the original exhibits placed in the bag. The bag is *not* intended to be used again for other exhibits.

Size

Presently, the Audit Bag is only produced in an A4 size, this being identified in 1984 as the optimum single size bag. Operational use of the bag since then, combined with proposals to extend the bag's use into other areas, has illustrated a demand for a variety of bag sizes from A5 to A3.

Cost per unit

In 1991, Audit Bags were being sold to police agencies at $2.05 per unit.

Patent Holders

The National Police Research Unit and Techsearch Incorporated jointly hold patents over the Audit Bag.

Manufacturer and marketing

The Audit Bag has been produced since the outset by Australian Vinyl of South Australia and marketed by 3M Australia.

Testing of security features and durability

During the development period of the Audit Bag, considerable effort was spent in testing the bag's 'defence mechanisms' to attack, principally to determine if any form of attack could allow the bag to be opened and resealed without visual or forensic detection. These tests, carried out by an independent laboratory not involved with the development of the Audit Bag, assessed the vulnerability of the bag to attack by insertion, cutting, chemical breakdown, freezing in liquid nitrogen and heating.

Preliminary testing revealed a number of weaknesses which were overcome by modifying the pattern and construction of the printed strip which bonded to the adhesive strip. The introduction of a hexagonal pattern to the printing made any access attempt quickly evident. Further, an extra weld was placed between each printed strip to stop insertion of tubes down the edge of the bag. In December 1986, the independent laboratory advised that each previously identified weakness had been successfully overcome.

During evaluations of the Audit Bag prior to implementation in New South Wales, concerns were expressed regarding the strength of the bag for holding sharp, heavy exhibits. To overcome this, the thermal welds of the bag were strengthened and a test protocol devised to conduct quality assurance testing. The test involves placing a 'Brickie's bolster' inside a bag and dropping it one metre to a dead stop. If the bag seams or seals fail, the batch fails. Such testing, whilst severe, does demonstrate the strength of the current specification Audit Bag.

Current usage

The South Australian Police Department has been employing the Audit Bag since early 1987 and reports continuing satisfaction with it. In that time, there has been no reported case of disputed evidence involving the Audit Bag. The New South Wales Police Service commenced issuing the bags in 1990, and in 1991 the Queensland and Victoria Police were undertaking trials.

Advantages of the Audit Bag

Evidence controls improved

The Audit Bag provides a facility whereby exhibits are placed in an accountable, tamper-resistant container at the immediate point of seizure. Upon return to the station, the supervising officer can visually check that the bag has not been tampered with since sealing. If necessary, further checks may be carried out by the supervisor opening the bag by cutting below the first seal, performing whatever checks are necessary (such as counting and weighing), and resealing the bag at the next adhesive strip. The accountable number of the bag and other details are entered in the exhibit receipt book and the exhibit stored or referred for scientific analysis.

Where scientific analysis is conducted, the analyst examines the bag to ensure no tampering since last sealing. If satisfied with the bag's integrity, the analyst opens the bag by cutting below the sealed strip, conducts the analysis and then reseals the bag with the next adhesive strip for return to controlled storage.

Exhibit audits may be conducted visually. Where degradation of the seal or other indicators such as plastic distortion may be evident, the exhibit can be referred for

scientific examination to confirm tampering prior to an internal inquiry being pursued further.

Less disputed evidence

Once evidence is sealed in the Audit Bag, the opportunity for claims of disputed evidence are significantly reduced. The control features surrounding the bag, combined with its inherent 'tell-tale' capacity if tampered with, offer tangible benefits to police administrators.

Of course, claims arising from the initial arrest or seizure point that the amount involved was more, less or 'planted' can only be overcome by ensuring that search, seizure, placement in and sealing of the Audit Bag are conducted, wherever practicable, by two or more officers and in the presence of the offender or suspect.

Whilst not quantifiable at this point, significant cost advantages are seen with the Audit Bag in reducing costs to police agencies in dealing with disputed evidence claims. The quite substantial costs involved in investigating such claims through to the very high cost of defending such claims in court may be reduced by the patent security inherent in the Audit Bag system.

Improving the professional image of policing

Equally, the professional image of the police agency can only be enhanced by presenting to court evidence stored in such a manner that tampering is impossible without being detected and investigated. Such professional 'packaging' must surely offer an improvement over evidence held in containers which are literally or metaphorically 'full of holes'.

Further, the implementation of secure exhibit systems has the potential for substantially removing the opportunity for and allegations of tampering with evidence after seizure. Through such police-initiated measures, the credibility of the profession will be enhanced.

Benefits will also accrue from reduced stress and other problems experienced by police officers facing unnecessary internal investigations or unsubstantiated courtroom allegations of impropriety.

Future Initiatives

Sizes

As mentioned earlier, users of the bags have expressed a desire for both smaller and larger bags in addition to the present A4 size. This demand is related not only to drug exhibits, as the bag is now being used for purposes other than exhibit security, most notably as property bags.

Number of seals

The number of seals required in a practical operational sense is also being constantly reviewed. As the seals represent the most costly production component of the bag, any feasible reduction in number will have tangible cost benefits to jurisdictions.

Bottom pocket

Equally, the NPRU has been advised that the added security intended through the bottom pocket may not be being exploited in practice. The necessity of retaining the bottom pocket is also presently under review.

Further Information

Further information on the Audit Bag may be obtained by contacting:

Mr Des Berwick
Executive Officer
National Police Research Unit
PO Box 370
MARDEN SA 5070

Telephone: (08) 363 3033
Fax: (08) 363 2164

RF RADIATION—FACTS AND FALLACIES

Ken Joyner*
Electromagnetic Compatibility Section
Telecom Australia Research Laboratories
Victoria

THE DEBATE OVER POSSIBLE ADVERSE HEALTH EFFECTS FOLLOWING exposure to electromagnetic radiation (EMR) is very controversial and very much to the fore in Australia today.

The Sir Harry Gibbs Inquiry into Community Needs and High Voltage Transmission Line Development in New South Wales and the debate on siting of the Richmond/Brunswick power line in Victoria have received a great deal of media attention.

EMR is a generic term and refers to the transport of energy in the form of an electromagnetic wave travelling at the speed of light. The EMR spectrum is very wide and covers power frequency fields, radio-frequency and microwave, infrared, visible, ultraviolet, X-ray and some nuclear radiations. (Note that, in the context of this paper, microwave radiation will be regarded as a subset of the radiofrequency (RF) band.)

Claims of adverse health effects due to EMR exposure include increased cancer rates, adverse pregnancy outcomes and cataract induction.

Insofar as police and law enforcement personnel are concerned, a possible risk due to exposure to EMR, over and above that of the general community, may arise because of the use of RF transmitting devices during the course of their employment.

In addressing the issue of increased risk of adverse health effects arising from exposure to RF, this paper shall draw heavily from the experiences of Telecom Australia, which is the largest user of RF radiation in Australia outside of the Defence Department. As such, Telecom Australia has a large number of people involved in the use and transmission of RF radiation with transmit powers as low as a few milliwatts up to several hundred kilowatts. A detailed discussion of the health risk management of RF radiation may be found elsewhere (*see* Hocking & Joyner 1991).

---

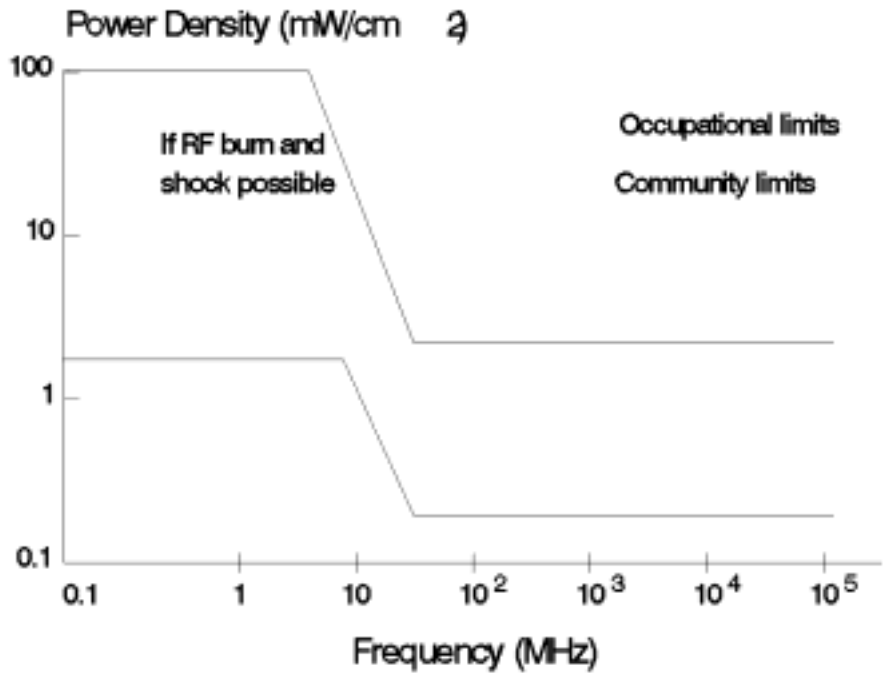
* I wish to express my thanks to Dr Trevor Boal and Mr Morrie Facci from the Victorian Health Department for much of the information on exposure levels from police radio equipment. The permission of the Executive General Manager, Telecom Research Laboratories, to publish this paper is hereby acknowledged.

Australian RF Exposure Standard

The allowable RF exposure limits in Australian Standard AS2772.1–1990 are shown in Figure 1.

Figure 1

Australian Standard AS2772.1–1990



Source: Standards Australia 1991, Australian Standard AS2772.1 Radio Frequency Radiation, Part 1: Maximum Exposure Levels, 100 kHz–300 GHz.

Several points about the Australian Standard are worthy of note.

- The time over which the measured RF level is to be averaged is sixty seconds. Obviously if an exposure takes longer than sixty seconds then the measured level is compared directly to the limit value. However, if an exposure takes only thirty seconds then the time-averaged exposure level is half of the measured level. For pulsed or intermittent RF sources, the time-averaged exposure level is found by multiplying the measured RF level by the duty cycle of the source. The duty cycle is the ratio of the time the RF source is on to the time it is both on and off.

- The exposure limits for the community are set at one-fifth of the lowest occupational levels in recognition of the fact that the general community encompasses babies, old people, sick and infirm persons and, those who, by virtue of living next to a transmitter site, may be exposed to the radiation for up to 24–hours a day.

- There is an exclusion clause in the Standard which exempts from compliance all devices which have output powers of less than 7 W and transmit frequencies of less than 1000 MHz.

Health Studies on Exposed Populations in Australia

Telecom Australia has conducted or contributed to two studies of the health status of its workforce. These are:

- All cases of neoplasms of the blood leading to invalidity retirement for the period 1 July 1976 to 30 December 1982 from the Australian Public Service and Telecom were obtained from the Australian Government Retirement Benefits Office. There were 119 cases of which twenty-five (21 per cent) involved Telecom staff. Of the 287,614 contributors, 28 per cent were Telecom staff. Analysis of the twenty-five Telecom cases did not show an over-representation of any work designation for leukaemia. Within the limitation of this study there is no evidence of Telecom operations causing an excess of leukaemia cases in staff (Hocking 1984).

- Chromosome studies were performed on blood samples from thirty-eight radio-linemen matched by age with thirty-eight controls, all of whom were employed by Telecom Australia. The radio-linemen had all worked with RF radiation in the range 400 kHz to 20 GHz with exposures at or below the occupational limits in the Australian Standard. The controls were members of the clerical staff who had no known exposure to RF radiation. Two hundred metaphases from each subject were studied and chromosome damage was scored by an observer who was blind to the status of the subjects. The ratio of the rate of aberrant cells in the radio-linemen group to that in the control group was 1.0 (95 per cent confidence interval, 0.8–1.3). There were no statistically significant differences in the types of aberrations that were scored. It was concluded that exposure to RF radiation at or below the limits in the Australian Standard did not appear to cause any increase in chromosomal damage in circulating lymphocytes (Garson et al. 1991).

Another study, independent of Telecom, was carried out by Hollows & Douglas (1984) who investigated the incidence of lens opacities in the eyes of Telecom radio-linemen. Hollows and Douglas examined with a slit-lamp the lenses of Telecom radio-linemen and age-matched controls. The exposed sample consisted of persons who had worked for fifteen or more years as radio-linemen and were over forty-five years of age but less than sixty years of age. The controls were mail sorters. The results of this study found that posterior subcapsular opacities occurred in 21 per cent of radio-linemen and 8 per cent of controls.

It is of interest to note that mail sorters require particularly good vision. In addition, a recent litigation case in Australia for cataract induction from occupational exposure to microwave radiation was lost by the applicant. The Administrative Appeals Tribunal found that:

> On the balance of probabilities, it is probable that the applicant's exposure to microwave radiation did not cause, or accelerate the development of, the cataracts or contribute to doing so (Joyner 1989, p. 548).

Exposure Measurements

Table 1 contains measurements of typical exposures for specific classes of equipment in use by police and law enforcement personnel in Australia. Many of the radios are not operated continuously and typically have a duty cycle of around 5 per cent. To find the time averaged exposure level the measured level should therefore be multiplied by 0.05.

As a general rule of thumb, for devices transmitting around 100 W a separation distance of 60 cm (an arm's length) is required to achieve compliance with the Australian Standard. Where possible, vehicular antennas should be located as far as practicable from occupants. Covert antennas should *not* be located in the head rests of vehicles.

Portable radios

Close to the antennas of devices operating below 1000 MHz and with output powers of less than 7 W, the measured levels can exceed the occupational exposure limits in the Australian Standard.

Even though these devices are exempt from compliance, questions have been asked about the legitimacy of the exemption given that exposure levels may exceed the limits. Very recent work at Telecom Research Laboratories has shown that the underlying basis for the exclusion clause is scientifically based and little or no thermal response is elicited in operators of exempt portable RF devices (Joyner 1989).

Portable radios that are not covered by the exclusion clause, such as high power backpack units, have to be treated on a case by case basis but, in general, the duty cycle of typical transmissions needs to be taken into account.

Radio maintenance

Technicians maintaining radio equipment should minimise exposures through the use of dummy loads and safe work procedures. Maintenance personnel should be involved in the formulation of the safe work procedures.

Table 1

Typical Exposure Levels for Specific Equipment Classes

Equipment Type	Antenna Mounting	Measured Exposure Level Relative To Limit
FALCOM Speed Radar Gun (24.15 GHz; 10–40mW)	Hand Held	0.4 @ 5 cm from aperture 0.3 through car windscreen not detected behind unit
UHF Radio (25 W)	Rear parcel shelf of vehicle	1.3 @ head of rear passenger (25 cm dist.) 0.13 @ head of driver 0.53 @ 40 cm outside of car adjacent rear door 0.19 @ 60 cm outside of car adjacent rear door
UHF Radio (25W)	Police motorcycle above rear wheel	0.7 @ rider's head 0.35 @ rider's waist 2.1 @ 15 cm from antenna
VHF Radio (20 W)	Police motorcycle above rear wheel	0.2 @ rider's head 0.13 @ rider's waist 4.0 @ 15 cm from antenna
UHF Radio (50 W)	Standard car radio antenna – passenger side	0.4 @ passenger's head 0.3 @ passenger's waist 8.0 @ 15 cm from antenna
PCM Hawk (100 W 4.78 GHz)	Rear of van driver's side	not detected inside van 17 @ 15 cm from antenna

Source: Author's own measurements plus measurements supplied by the Radiation Section, Department of Health and Community Services, Victoria.

Conclusion

A number of conclusions can be drawn from the previous discussions. These are:

- there do not appear to be any serious health problems caused by exposure to RF radiation at or below the recommended limits in the Australian Standard;
- the RF exposure levels to which police and law enforcement personnel are exposed are, in general, lower than the recommended limits in the Australian Standard;

- vehicular antennas should be mounted as far as is practicable from the occupants of the vehicle. Covert antennas should not be placed in the head rests of vehicles; and

- specific operational procedures may need to be introduced with the use and maintenance of some equipment in order to ensure compliance with the Australian Standard.

References

Garson, O.M., McRoberts, T.L., Campbell, L.J., Hocking, B. & Gordon, I. 1991, 'A chromosonal study of workers with long-term exposure to radio frequency radiation', *Medical Journal of Australia*, no. 155, pp. 289–92.

Hocking, B. 1984, *Neoplasms of the Blood*, Occupational Health Services, Paper No. 6, Telecom Australia.

Hocking, B. & Joyner, K.H. 1991, 'Health risk management of radio frequency radiation', *Journal of Occupational Health & Safety: Australia and New Zealand*, vol. 8, no. 1, pp. 21–30.

Hollows, F.C. & Douglas, J.B. 1984, 'Microwave cataract in radiolinemen and controls', *Lancet*, no. 2, p. 406.

Joyner, K.H. 1989, 'Microwave cataract and litigation: a case study', *Health Physics*, no. 57, pp. 545–9.

Joyner, K.H., Lubinas, V., Wood, M.P., Saribalas, J. & Adams, J.A. 1992, 'Radio frequency radiation (rfr) exposures from mobile phones', *Proceedings of the IRPA (Intensification of Research in Priority Areas) 8th World Congress*, Montreal, May 17–21.

Standards Australia 1991, Australian Standard AS2772.1 Radio Frequency Radiation, Part 1: Maximum Exposure Levels, 100 kHz–300 GHz, North Sydney.

INVESTIGATIVE SKILLS FOR THE 1990S AND BEYOND

David Thompson
Detective Sergeant
Fraud Squad (Computers)
Victoria Police

Computers: The New Criminal Modus Operandi

COMPUTER CRIME, HIGH-TECH CRIME, AND COMPUTER FRAUD ARE ALL terms used to describe the involvement of computers in the commission of crime. Computers have become a common business and household item and come in the form of personal organisers, notebooks, laptops, desktops, networks, mini and mainframe computers. Computer technology has not introduced a new crime but has changed the form of traditional commercial-type crimes. Committing crimes by computer can be viewed as a new modus operandi in the commercial crime field. Crimes that were once committed with pen and paper are now often committed in a computer environment.

Due to the changing form of business information systems, investigators are experiencing a substantial increase in the amount of computerised information forming part of current investigations. This information ranges from complainants' computerised company records to the seizure of suspects' computers and computerised records.

Since 1980, the form of business information systems has changed substantially. Many organisations now operate some form of computerised information system ranging from word processing to entirely paperless trading (which involves only computerised transactions and documents).

Investigators' Skills

No longer do commercial crime investigators only require an understanding of accounting and business practices to perform their job. They must also have an understanding of computer technology and business information systems in order to identify and gather evidence during investigations. It is now necessary for detectives to be computer literate enough to competently search and seize computerised information systems (particularly personal computers). Investigators also require

sufficient skills to analyse and identify information of evidentiary value from typical computerised business records.

Changes in Investigative Skills and Practices

This changing form of commercial crime has highlighted some deficiencies in the existing investigative practices, skills and knowledge of investigators who are required to deal with crimes involving the latest business technology. The investigative skills and practices of the law enforcement community have changed little over the past few decades. Until the 1990s, little attention had been paid to the impact of computer technology on the nature of business information systems—particularly the impact that computer technology has had on the ability of detectives to search, seize and analyse documentary evidence.

The computerised document has had a significant impact on the investigator's ability to prove the identity of offenders who have used documents to commit crimes. No longer are fingerprints, handwriting, typewriter analysis (although limited printer analysis is possible), indentations or pen striations able to be used to provide a nexus between the criminal and documents used to commit crimes involving computers.

Many experienced investigators have limited computer literacy. In fact, some of these investigators believe that there is no need to improve or develop new skills because they have never required specialist technical knowledge in any other field in order to investigate crimes. The fallacy in this argument is that, for centuries documents have been recorded on paper, and now documents are being created and stored on computers—even to locate and read a document requires some computer knowledge. Greater knowledge is required to successfully preserve, search, seize and analyse typical computerised business records and systems.

In order to efficiently and effectively conduct investigations in the commercial environment, investigators' skills and knowledge must keep pace with the technological changes in the general business community. It is essential that law enforcement agencies recognise the need to keep abreast of these changes and implement strategies to develop new skills, knowledge and work practices related to current business technology. It is also essential that computer technology is used to aid investigation for two reasons: firstly, to support the processing of information related to an investigation; and secondly, to actually facilitate the conduct of an investigation in the computer environment.

Use of Computer Technology to Aid Investigation

Due to the nature and complexity of commercial crimes, it is very time-consuming to record, store, retrieve and analyse information relating to investigations. It is in these tasks that the use of computers by investigators will provide more accurate and efficient handling of documents and information and a more cost effective use of equipment and resources. Some of the major functions for which computer technology can be used to support investigations are:

- case management systems for investigation and administrative data;
- preparation, storage and retrieval of briefs of evidence and other documents related to investigations;
- analytical and intelligence systems to support investigations;
- access to the police and other government agency on-line computer systems;
- access to other relevant external on-line computer systems;
- use of portable computers in the field; and
- use of application software to support investigations.

Case management systems

A computerised database of information relating to investigations should provide an ability to store and retrieve information relating to complainants, suspects, victims, witnesses, businesses, addresses and other relevant information. The information known by an investigator is of great importance to other personnel in both the administrative and investigative roles.

An efficient and effective case management system will not only provide important administrative information, it will also be an investigative aid by providing historical and current information about investigations, which are not easily identified or retrieved from manual information systems.

Preparation of briefs of evidence

The process of preparing and storing information relating to briefs of evidence should also be computerised. All statements, witness lists, exhibit lists, informations, spreadsheet charts, graphs and database records should be stored on computer for easy retrieval, amendment and compilation of briefs of evidence for prosecution. This procedure enables all relevant information on a particular investigation to be efficiently controlled and easily located by members requiring access.

Standardised forms such as witness lists, exhibit lists, informations for an offence and warrants can be created. This will enable word processor operators or data entry staff to produce standardised documents for briefs of evidence, and release detectives from the task of preparing their own proformas during an investigation. The ability of micro-computers to expedite time-consuming tasks performed by detectives (such as typing and collating) will now allow detectives to spend more time actually investigating.

Intelligence and analytical systems

Analysis of collected and stored information can be used to identify similarities in cases; this may identify suspects and offenders for offences with no known suspects. Offences can be analysed and grouped using details such as modus operandi, suspect or car descriptions to aid the apprehension of the offender.

Analysts can provide accurate and current information on known suspects, offenders, premises and vehicles to assist in the identification of offenders responsible

for unsolved offences. This is done by searching the profiles of known persons and identifying all the offences in which particular suspects or offenders were involved.

There is a need for an intelligence and analytical function to support investigation of complex crimes which typically involve numerous associations between persons, companies and business transactions. The preparation of link analysis charts and association matrices are valuable aids to investigators during complex investigations.

Access to police and government on-line systems

There is a need for access to police and other government agency computer systems. Investigators have had access to computerised information such as criminal records, motor vehicle and licence details for over a decade, which has proved to be a valuable resource during their investigations. It is now time to integrate local personal computing resources with other police and government systems. Access to these systems will enable investigators to use corporate and government data, which can be analysed locally, to assist investigations.

External computer systems operated by other government agencies—such as the Cash Transactions Reporting Agency (CTRA), the Australian Securities Commission (ASC) and the Titles Office—will be of substantial benefit to investigators in the task of tracing financial and other paper trails. The opportunity to access these systems is readily available, others may require negotiation with the appropriate government departments.

Access to other external computer systems

With the increasing availability of publicly-accessible on-line database systems, the opportunity for investigators to remotely access other external computer systems will also provide a valuable investigative resource.

Portable computer facilities

There is a need for access to portable computing facilities to support investigations conducted away from the office. The ability to type statements obtained from witnesses directly into a computer in the field will eliminate the double handling of handwritten statements which have to be typed on return to the office. Where numerous documents are required to be handled, a portable computer could be used by investigators to transport all the necessary information required to conduct their inquiries—such as a full copy of exhibits, statements, database information and other relevant files. Without the assistance of information stored on computer, detectives will very often be confined to the office when interviewing witnesses because it is not practical to transport all the documentary evidence to a witness' premises.

Communication from the field using a portable computer via modem access to the telephone network will enable access to the computer facilities of the investigator's office. This will save time as it will no longer be necessary to return to the office to obtain additional information required during an investigation. Modem access would enable communication with the office from local, country, interstate and overseas locations.

Use of application software to support investigations

Computers can be used as an aid to investigations by performing the following functions:

- the use of databases to record, collate, and analyse exhibits, financial transactions and other documents;
- production of spreadsheets of financial data relating to investigations;
- the use of text retrieval software to analyse textual information relating to investigations;
- production of graphical representations such as flow charts, graphs and other images as an investigative aid and for ultimate production in court;
- the use of optical scanning technology to reproduce image or textual documents for analysis or presentation at court;
- the use of geographical mapping software to map known locations of suspects or incidents;
- the use of hypertext software to allow the linking and analysis of information collected during an investigation, in a manner not bound by the structure of database systems; and
- the use of expert systems to provide a standardised manner to perform tasks requiring expert or specialist knowledge.

Database software: Due to the volume of information collected during a commercial crime investigation, it is a very difficult and time-consuming task to sort and collate documents for analysis and presentation at court. It is essential that any information and documents—such as cheques, invoices, and other financial or business records—are collated and analysed in differing sequences to identify items of evidentiary value and to determine what offences have been committed. The task of analysing and collating exhibits can often take many months, due to the cumbersome and repetitive nature of this task.

With the aid of computers this information can be input into a database and the analysis of this information can be completed in a much shorter time span. Although time must be spent entering information into the computer, this task could be undertaken by data entry staff. The benefit obtained by entering this type of information into a computer is that it may be resorted and queried many times with the results being available immediately. The computerisation of some investigations can save many months of repetitive manual sorting, resulting in the early apprehension of offenders.

Spreadsheets: A spreadsheet, or ledger sheet, is primarily used in business by accountants for performing financial calculations and recording transactions. An electronic spreadsheet is simply a computerised version of a traditional spreadsheet. Spreadsheets can be used to analyse financial or other numerical data collected during investigations. They can also be

used to view and analyse the computerised records of victims or suspects seized during an investigation.

Text retrieval software: Text retrieval software can be used to search and analyse existing word processed documents such as statements, exhibit or witness lists, intelligence reports, warrants and investigation logs which are created during the course of investigations. It can also be used to analyse paper documents which have been optically scanned (OCR) and stored as text files, or computerised text files seized or obtained on computer storage media during an investigation. The documents can be searched for specific words, phrases or similarities which can then be retrieved for viewing, copying and manipulation. The text of a document can be manipulated in a word processing environment and then exported for input into a database or spreadsheet for sorting, query or further analysis.

Graphic representation: Graphics software packages can be used for the production of graphs and charts, and the summarising of data for presentation purposes. They can be used for presentations on monitors or can be printed for distribution. The printed output from these packages can also be used to create slides or transparencies. These different forms of output could be used for briefings, analysis and to assist the presentation of evidence in court.

Graphical representation of financial transactions has proven to be an extremely useful aid during investigations and in presentation of complex transactions to the courts. This process can now be performed using computer graphics technology which is far more efficient than the previously hand-drawn charts. The cost savings and flexibility of altering computer-generated presentations during investigations or court hearings have been demonstrated in a number of recent cases.

It is now possible to use personal computer charting programs to create graphic charts. It would be of benefit to investigators to be able to use a computerised charting facility during investigations to depict financial information and other link analysis charts. This facility is an essential aid to the investigation of complex commercial crime matters which will replace the hand-drawn charts currently used. The charts drawn by the investigators could then be used as the basis for the final charts prepared for court presentation.

Optical scanning of documents: The time-consuming task of keying documents into a computer can be further expedited with the assistance of a digital scanner using image or optical character recognition (OCR), software which optically scans a document and stores a copy of it digitally. The documents can then be retrieved to enable viewing of graphical images such as cheques, or the searching or manipulation of textual data. This facility would be of value where numerous exhibits are scanned as images and appended to a database for sorting, analysis and viewing. The computerised image could then be shown to witnesses and reproduced for inclusion in briefs of evidence. Ultimately, optical scanning can be used as an aid in the presentation of exhibits to the court.

Hypertext software: Because the process of investigation is not an organised and structured process, the use of database management software to organise data collected during an investigation can be restrictive when trying to establish links and associations. The use of hypertext software to link and analyse information collected

during an investigation is a viable alternative, due to the fact that hypertext is not bound by the structure of typical database systems. Hypertext type software will generally allow the operator to make links and associations as required. This could be very useful for intelligence analysis and investigative functions.

Geographical mapping software: The task of collating and analysing the locations and geographical relationships between offences can be aided by the use of geographical mapping software. The locations of suspects or incidents can be entered or imported from other computer systems to allow geographical analysis and presentation by investigators.

Expert systems: There is an opportunity for the use of expert systems in the investigative function. These systems use 'deductive reasoning' which is the same process that investigators use to solve crimes. The prospect of using computers which are able to process information at much faster speeds than humans, and the ability to reference much larger databases of information, is likely to greatly enhance an investigator's ability to solve crimes. These systems could provide the skills and knowledge of the most experienced investigators in the entire organisation. What must be remembered is that an expert system will not replace investigators, but it will assist them to perform more effectively and consistently. Expert systems could be used to support investigations in the following areas:

- an investigator's notebook that tracks and maintains a log of all actions taken during an investigation, including all inferencing, evidential reasoning and 'what if' capabilities;

- on-line intelligent access to existing databases;

- assist in criminal profiling of offenders by identifying major personality and behavioural characteristics and analysing the crime scene and other related evidence; and

- link analysis to identify relationships between persons and then make deductions about other relationships in order to assist the investigation.

Use of computer technology to conduct investigations

As commercial crime offenders are known to often use the most advanced technology available to support their criminal activity, it is now necessary for investigators to use similar technology in their efforts to investigate this form of crime. Commercial crime investigators are currently finding computer facilities located at many of the premises being investigated. The evidence that is being sought is often located in a computer environment which requires the use of computer equipment and software to facilitate search, seizure and retrieval. If investigators are to be successful, they must not only understand the technology but must also have access to it as an investigative tool.

Computers: The New Investigative Tool

Investigators require access to computer hardware and software to assist in the conduct of investigations. The investigative computer functions can be broadly categorised as follows:

- search and seizure of computers and computer storage media;

- analysis of computer evidence; and

- interception and monitoring of data communications.

The recovery of data from computers is a new law enforcement speciality. Some law enforcement personnel consider it a new Forensic Science which requires knowledge of the laws of search and seizure, rules of evidence and extensive computer knowledge (Stites 1990).

Search, seizure and analysis of computer systems

Criminal investigations involving computers and related technology require hardware and software to support the search, seizure and analysis of evidence obtained. Evidence obtained cannot usually be viewed or analysed without the aid of computer hardware and software. In many cases the evidence obtained may be from a system that is not compatible with the standard police equipment used for analysis. Therefore, investigators require access to a variety of computer hardware and software (application and operating system) or equipment that will allow the conversion of information from different environments and types of computer storage media.

Many software packages—such as industry standard application software packages, audit utility software, virus detectors, operating systems, utility programs and decryption programs—are required by investigators to aid the search, seizure and analysis of computers and computer evidence seized. These software utilities are used to access, copy and analyse data seized or identify deleted or 'hidden' files used by

offenders to hide evidence from investigators. In many cases files which are 'hidden' or erased can be retrieved by using these special utilities. These packages also provide the facilities for a detailed analysis of the computer system configuration which is of importance to the investigator.

Interception and monitoring of data communications

Due to the fact that many offenders utilise telephones, computers, beeper messaging systems and facsimile machines to conduct their criminal activity, the use of equipment to intercept these communications will be extremely useful in associating suspects with transactions where there is no personal contact with victims or other involved parties. The sophisticated equipment to monitor and intercept these devices is currently available and is going to become essential as transactions continue to become computer and telecommunications-based.

Access to current technology is urgently required by investigators in this technologically-complex field. It is important to recognise that technology-related crime is based in a rapidly changing environment. The tools used to combat it must be continually evaluated and regularly upgraded to ensure that the most efficient and effective use of resources is achieved.

Whilst the use of computer technology will provide the means to identify and gather computer evidence, it is essential to develop policies and procedures to ensure consistency in investigative practices in order to preserve originality, continuity and admissibility of gathered computer evidence. These practices and guidelines can be presented to investigators through new training programs relevant to this field.

Development of Investigative Computer Skills and Practices

Computer application software training

In order to effectively use computers to support investigations, investigators should at least understand the operation of personal computers and develop proficient skills in the use of application software, such as word processing, databases, spreadsheets and any other relevant packages. These skills will be a sound base for the development of the computer investigative skills required to use the computer to conduct investigations involving the search, seizure and analysis of computers and computer evidence. Before attempting to develop computer investigative skills, investigators should have gained some initial computer literacy. This can be gained from a training program on the introduction to personal computer operations and application software use.

Investigative computer training

The computer training of investigators should be based on the nature of offences they will be expected to investigate. The nature of the offences are best categorised by the degree of technical expertise that may be used by offenders to commit computer-related crimes. The nature of computer crime can be classified into three basic technological categories (identified by Federal Bureau of Investigation research in the USA):

- computer operations (input, output);
- programs and data (processing); and
- systems and communications (environment and transmission).

A training program for investigators in this field should separately address the degrees of technical skill with separate levels of training. The training program should only attempt to address the first two categories of technical expertise because the third category is an extremely technologically-complex domain which should be left to specialist computer professionals (who can be utilised as consulting experts).

Training program structure

The skills required can best be provided by a three-tiered training program which is provided to detectives in progressive phases, based on their specific investigative function.

- Level 1 — Awareness Skills (theoretical): this level is not related to the technology categories, but is a prerequisite for Level 2 training;
- Level 2 — Broad Knowledge (theoretical and practical): to address the skills required for investigations involving computer operations (input, output) (Technology Category 1); and
- Level 3 — Sound Knowledge (theoretical and practical): to address the skills required for investigations involving program and data manipulation (Technology Category 2).

The training program should provide the opportunity to present the skills required by the generalist investigator through to the specialist computer crime investigator. All investigators should at least have a theoretical awareness (Level 1) of the technological issues that apply to an investigation in the computer environment. Detectives assigned to specialist commercial crime duties (such as the Fraud Squad) should have a broad understanding of computer technology issues (Level 2), with theoretical and practical expertise in the personal computer environment. Specialist computer crime investigators should have a sound understanding of computer technology (Level 3) to enable them to undertake complex technological investigations in all environments (with or without consultant experts).

It is not suggested that all investigators require an extensive knowledge of computers (although this may be the case in the future), merely a sound understanding

of computing principles and practices in relation to small computer systems (personal computers) used by most businesses today.

Specialist computer training

Whilst the three-tiered training program should cater for most skills and knowledge required by investigators at different levels, there will be occasions when additional skills and knowledge will be required by investigators, particularly those who have completed the full training program. Provision should be made for ongoing training of the members involved in the specialist investigative computer analysis function to ensure that their knowledge and skills are maintained.

The nature and extent of training in this field will become an important factor in determining whether the law enforcement community will have the capacity to efficiently and effectively investigate modern commercial crime.

Research and development of computer investigative techniques

Although the methodology for the investigation of technological crime is based on general investigative procedures, the technological components require a renewed approach involving the development of new techniques and use of new equipment. In 1991, the law enforcement community in Australia does not have access to advanced techniques to aid in the retrieval, seizure or analysis of computer evidence.

A number of investigative procedures and techniques for search, seizure and analysis of evidence in the computer environment using standard industry tools have been developed. Yet there is a need for more advanced techniques to be identified and used to support investigations involving the analysis of evidence from computer environments. Some of the areas which need to be addressed are :

- the conversion of computerised evidentiary information from differing storage media and formats to a form which is compatible with the systems being used by investigators for analysis;

- the analysis and comparison of electronic and computer printed documents to determine characteristics of an evidentiary value;

- the analysis and retrieval of data or programs which have been deleted, changed, hidden or encrypted on computer storage media; and

- the development of specialist computer software utilities to aid the search, seizure and analysis of computer systems and data.

A Example of a Computer Training Program

The Victoria Police Fraud Squad conducts a three-tiered computer training program which is consistent with the model discussed. The three levels of training are provided to detectives in progressive phases which provide the knowledge and skills required for their specific investigative function. The computer training program consists of the following three levels:

- Economic Crime Course, computer segment (theoretical);
- Business Systems for Investigators Course held at the Royal Melbourne Institute of Technology (RMIT) (theoretical and practical); and
- National Computer Crime Investigators Course, held annually (theoretical and practical).

Economic Crime Course, computer segment

The Fraud Squad Economic Crime Course (general training course) currently provides theoretical instruction on the investigation of crimes in the computer environment as part of the syllabus (equivalent to Level 1 training). This segment is aimed at new members of the Fraud Squad or those with limited fraud investigative experience. This component broadly covers the following topics:

- introduction to computer technology and terminology;
- legislation related to crimes involving computers;
- evidentiary legislation and issues; and
- investigative procedures and practices.

Business Systems for Investigators Course

This advanced training course has been implemented to provide the skills necessary to bridge the gap between the Economic Crime Course and the current National Computer Crime Investigators Course. This course provides the knowledge and expertise required to search and seize a personal computer in order to gather computer evidence. The course aims to provide the following skills and knowledge to participants:

- familiarity with the major features of computer systems sufficient to determine the difference between small and large computer systems;
- the ability to recognise and use the basic features of generic computer software packages used by businesses;
- the ability to identify and recognise software package-related characteristics of files and data used on personal computers;

- the ability to identify and recover computerised data stored on a personal computer which is required as evidence, without damage;

- familiarity with the basic terminology, tools and procedures used to examine computers and computer storage media; and

- practice in the investigation of small computer systems using standard tools and investigative procedures for identifying and gathering computerised information.

This structure is similar to a typical tertiary subject presentation and is considered the best approach to ensure maximum comprehension and retention of the information and skills presented. The duration, course content and method of assessment is consistent with the subjects taught in other business computing courses at tertiary level.

The content of the training course satisfies the prerequisite level of training required for the National Computer Crime Investigators Course. This will provide a pool of investigators from which to annually select members who are suitable to go on to more advanced computer crime training.

National Computer Crime Investigators Course

The National Computer Crime Investigators Course aims to provide a sound knowledge of computer technology and the investigative techniques and procedures required to investigate complex crimes in the computer environment. The objectives of the course are to:

- provide an overview and definition of crimes in the computer environment;

- provide knowledge of the current and emerging technologies, procedures and practices being used by the business community in the computer environment;

- provide a knowledge of the investigative techniques, procedures and practical skills required to investigate complex crimes in the computer environment; and

- provide a knowledge and understanding of the law and prosecution procedures related to crimes in the computer environment.

The Future

According to law enforcement futurists, as law enforcement focuses its attention on the traditional crimes (those with which it understands and is equipped to deal with) computer crime is emerging as a threat to the economy and national security. What may be portrayed as a sudden and dramatic increase in high technology crime has grown steadily for a decade and largely been ignored (Tafoya 1987). It is predicted that the law enforcement community could be overwhelmed by technologically-sophisticated crime and may be reduced to taking preliminary reports while the

investigations are conducted by private organisations of contracted specialists (Temby & McElwaine 1987).

The failure of the law enforcement community to recognise the problems and provide adequate technical skills and facilities for investigators may have a substantial effect on our ability to deal with this form of crime. The law enforcement community must recognise the problem and understand the techniques and technology that may be employed. If investigators fail to provide an appropriate and effective response to crimes involving technology, they will be compelled to endure the future by failing to shape its course (Tafoya 1987).

The important issue to be recognised in relation to computer crimes is that they are coming to notice more often. The law enforcement community must prepare itself to deal with the investigation of commercial crime which will soon be extensively computer-based. In a report to the USA Congress in 1990, William Sessions, the Director of the USA Federal Bureau of Investigation stated that:

> in the continuing fight against computer crime, the law enforcement community must continue to strengthen its investigations, training and support services (Sessions 1991, p. 13).

A failure to address these issues may confirm the futurists' predictions.

References

Sessions, W.S. 1991, 'Computer Crimes: an escalating crime trend', *FBI Law Enforcement Bulletin*, vol. 60, no. 2, February, pp. 12–15.

Stites, C.M. 1990, 'PCs—Personal Computers or Partners in Crime?', *Law and Order*, vol. 38, no. 9, September, pp. 161–65.

Tafoya, W.L. 1987, 'Into the Future . . . a Look at the 21st Century', *Law Enforcement Technology*, September/October.

Temby, I. & McElwaine, S. 1987, 'Technocrime—An Australian Overview', *Criminal Law Journal*, vol. 11, no. 5, October, pp. 245–58.

THE FUTURE OF FORENSIC SCIENCE

James Robertson*
Assistant Secretary and Head
Forensic Services Division
Australian Federal Police
Australian Capital Territory

IN PREPARING THIS PAPER I AM MINDFUL OF THE FACT THAT THIS Conference is focused on technology and that delegates will probably have an expectation that I will discuss new equipment and perhaps do some 'crystal ball gazing' with regard to new forensic techniques. However, this paper will address the application of technology to problem solving and, in particular, what information value can be gained from a particular analysis. Thus, while this paper shall touch upon what the future might hold for forensic science, the main focus is unashamedly on the future viewed from a more philosophical viewpoint.

In order to look to the future it is necessary to analyse the present. Where is forensic science today and what are the real issues confronting its practitioners? One only has to look at recent headlines in the print media to gain some insight into these issues, and it is suggested that there are four major issues confronting forensic scientists:

- organisational structures;
- independence;
- the legal system; and
- standards.

* The views expressed in this paper are those of the author alone.

Organisational Structures

No two states in Australia have an identical organisational structure for their forensic services, and only South Australia and Victoria have laboratories which offer a comprehensive service in an integrated facility. Changes to existing structures are being considered in most, if not all, of the remaining states. Specifically, a new forensic biology institute is planned for Queensland, which is also undergoing rapid civilianisation of its police forensic areas. A review committee is currently considering the future organisation of forensic science laboratories in New South Wales and the New South Wales police force has recently completed a major review of its physical evidence or crime scenes group.

In predicting the future, it is highly improbable that a unified approach—along the lines of the Home Office system in England or the Royal Canadian Mounted Police system in Canada—will emerge in Australia. The federal nature of Australia and the differing histories of the states work against such a system developing. Each jurisdiction will make up its own mind what will work best. There seems little doubt, however, that there is general agreement that forensic science laboratories should be independent of other agencies involved in the legal system such as the police and Directors of Public Prosecutions or Attorneys-General Departments. For example, in New South Wales, the proposed Forensic Science Institute will answer to an independent authority. In South Australia, State Forensic Science is part of the State Services Department.

An ideal model would be for forensic laboratories to be associated with a university in a symbiotic relationship. The university would receive rent for premises, have access to scientific research with a social value while the forensic laboratories would benefit from being part of a larger group with access to library facilities, expertise and equipment which might be too expensive, or where its use would be too infrequent to justify purchase by the laboratory on its own. Staff would also be able to form cooperative links with academic staff and students would be available for project work. The potential benefits could be enormous.

However, the forensic laboratory in Victoria is part of the Victoria Police, as is the Forensic Division of the Australian Federal Police (AFP). The Metropolitan Police laboratory in London is one of the most respected forensic laboratories in the world, and the Royal Canadian Mounted Police (RCMP) also have a highly respected series of forensic laboratories. Does this mean that these organisations are wrong? The answer is a definite NO and this opinion is based on the author's ten years' experience in academia, five years' in State Forensic Science in South Australia, appearances numerous times as a defence witness, and as a manager within the Forensic Services Division of the AFP.

In the Forensic Services Division of the AFP, the benefit of being part of a police department is that the Division has carriage for the complete forensic investigation from the scene examination to the completion of the scientific examination. The key to making this work successfully is having appropriately qualified people in the right positions. The unified workforce of the AFP has also been a key factor, as it means members and staff members have virtually equal pay and conditions, and these are issues which can cause problems in police departments between sworn officers and civilians. The importance of clearly defining the roles and responsibilities of each group in the Division cannot be overstressed. People need to understand what part they play in the overall investigation. When this works well, it is an organisational structure which is difficult to beat. There is, however, the argument of independence.

Independence

The independence of forensic scientists, both at an individual level and that of organisational structures, has been widely questioned. The aim of any credible service agency is to provide objective, impartial advice which can be relied upon by the court. How this is achieved at the organisation and individual level is the challenge.

It could be argued that a forensic area within a police force cannot be independent. This assertion could be disputed. It is an easy criticism to make against police that their investigations are sometimes less than even-handed and open-minded. (It is beyond the scope of this presentation to present the evidence for or against this assertion.) It is, nonetheless, the author's firm view that police are far less guilty of these shortcomings than would be the view of some players in the adversarial arena—police are easy targets for criticism. This is not to diminish in any way the need to maintain an awareness of the potential to be less than thorough, even-handed and open-minded. However, it is suggested that working from within a police environment, it is possible to influence the way in which colleagues think and act. However, this paper will not pursue this aspect further as what is important is to enunciate the need for forensic scientists to face up to the criticisms that they are in some way lackeys of the system and acknowledge the fact that, unless they take a more public stance to defend themselves, these perceptions will become self-fulfilling.

To borrow from a document produced by the AFP Intelligence Division, information has four elements:

- fact;
- opinion;
- rumour; and
- inference.

It seems that many of the facts about forensic science—as espoused by non-forensic scientists—are based on ill-informed opinion, based on rumour and with far from rigorous analysis and inference. In an editorial in *Science* titled 'The Willingness to Risk Failure', the author concluded that:

> A willingness to accept the risk of failure is one of the costs of leadership and, therefore, the price of all success (Shapiro 1990, p. 609).

Forensic scientists, indeed scientists in general, have not been noted for taking risks in entering philosophical debates on issues which affect their lives. Most of the 'opinions'—the erudite statements—are made by other players in the game. The hope for the future is that, as a community, forensic scientists can find a more effective voice to balance the books.

To return to independence, within an adversarial system it is seriously doubted that whatever or wherever the forensic organisation *sits*, defence lawyers will be reluctant to have work done in the same laboratory as police evidence. It would be good to see a laboratory which is completely independent of any prosecution work, perhaps as part of a university teaching department, and it is encouraging that an undergraduate program in forensic science is planned at the University of Technology, Sydney.

The Legal System: Jury/Adversarial Problems

Much debate has centred around the adequacy or inadequacy of the jury to understand scientific or expert evidence, and some commentators have gone as far as to say that 'the resolution of scientific disputes must be taken out of the courtroom' (Lloyd 1991, p. 2).

There has been much talk of miscarriages of justice and forensic scientists being castigated for errors. Certainly there is no room for a complacent response from forensic scientists. In fact, there has been very little response at all from forensic scientists! For whatever reason, this is another example of the profession not tackling the hard issues and in the author's opinion, a lack of leadership in senior ranks.

One way or another, as a group, forensic scientists must find a way of making a meaningful contribution to this debate. The jury system is capable of dealing with scientific evidence. However, forensic scientists do need to look hard at their in-court scientific evidence presentation skills; the court aspect is, after all, what makes one a forensic scientist as compared to any other scientist. It is suspected, perhaps unfairly, that too many forensic scientists do not see the business of going to court as a major aspect of their work. There are many reasons why mistakes may occur in court. Forensic scientists are only one side of the equation and very much the small part. Kevin Borick, President of the Australian Criminal Lawyers Association, has commented in a letter published in the *Weekend Australian* (26–27 October 1991) that these reasons include:

- complex and confusing laws;
- outmoded procedures;
- inadequate professional training of judges and lawyers; and
- an underfunded legal aid system.

Perhaps if the legal fraternity were more informed and educated in forensic matters, scientific evidence would be dealt with more effectively in court with less chance of jurors drawing the wrong conclusion or attaching the wrong weight to the evidence. It is up to all those involved in the legal system to try and make the existing system work better.

Standards

The key to solving many aspects of the problems raised in the preceding sections of this paper lie in this final issue of standards. What does the future hold in store? It does not take a particularly astute observer to work out that in the 1990s forensic laboratories will move towards accreditation. State Forensic Science in South Australia has set the example by successfully gaining accreditation from the American Society of Crime Laboratory Directors (ASCLAD) and other laboratories will follow. The ASCLAD system looks at quality management and the National Association of Testing Authorities (NATA) in Australia also have a broad-based program which tests quality systems based on ISO9000 series guidelines. It may be that a model incorporating the two systems will develop in Australia.

The value in the accreditation approach is that it tests the whole organisation and its demonstrable commitment to staff and standards. It does not necessarily follow that the laboratory will be doing the most appropriate tests or that individual workers are competent—these issues need to be addressed in other ways.

Two other groups will play important roles in addressing accreditation issues: the Specialist Advisory Groups (which exist under the mantle of the Senior Managers Australia and New Zealand Forensic Laboratories (SMANZFL) group) and the soon to be established National Institute of Forensic Sciences (NIFS). NIFS has the potential to influence, in a highly positive way, the development of the subject across the board from the police technical level to forensic science laboratory.

The issue of accreditation of individuals, especially those who operate outside of major laboratory systems, is a more difficult matter. There may be a role here for a professional body such as the Australian and New Zealand Forensic Science Society. However, this is some way in the future. The 'profession' has a considerable need to develop further before it takes on the issue of accreditation.

A final contributor to standards is education. In the AFP, the Forensic Services Division has made a major commitment to training and education, establishing, through the Australian Capital Territory College of Technical and Further Education (TAFE), an Associate Diploma in Applied Science/Forensic Investigation. Many police forces are well-underway in introducing similar initiatives. The future must see a greater degree of professionalism for police technical officers.

One word of caution against this optimistic view. Increasingly, the staff of forensic laboratories are becoming more specialist. The introduction of DNA testing has meant that a degree in molecular biology is almost a prerequisite for entry to the biology section of larger laboratories. Consequently, the role of the generalist has decreased in recent years. Certainly today's scientist needs to have an indepth knowledge of his or her subject, and perhaps it is now impossible to keep a broad base of expertise. However, it is fair to say that there is a much narrower set of skills available in laboratories in 1991 than in the 1980s or 1970s. This narrowing of skills is unlikely to be beneficial in the long term, and it is hoped that decision makers have the long-term foresight to ensure a balanced view to staffing. Once skills and knowledge are lost they are difficult to recover. Many forensic skills are like rare species, still existing in isolated pockets but under threat of extinction.

Conclusion

This paper has attempted to look at the future from what are perceived to be the issues which need to be addressed by the forensic community in the next ten years. There is much about which we can be positive and optimistic.

New technologies and improved instrumentation will continue to emerge. Forensic science usually has a lag period before these are adopted into the forensic arena, and this is to be expected, given the conservative nature of the legal arena. In the past, however, the lag period has been too long. Forensic scientists need to be quicker to recognise the potential applications to forensic problems and they also need to be able to carry out research aimed at helping to interpret what analytical data means.

Above all else, forensic science is an information subject. The power of technology has far outstripped forensic science's capacity as a subject to fully utilise the data available. For example, in 1991 the major approach to DNA being used in laboratories involves the use of so-called *single locus probes*. The potential discrimination offered by this approach is enormous, with figures of one in several million often quoted. There has been considerable discussion in scientific literature and in the popular press regarding the issues surrounding the use of this data. However, assuming the analysis is beyond criticism, the fundamental difficulty has been in presenting these figures in court, where arguments have centred on population genetics. For this and many other compelling reasons, the single locus approach will be replaced by the application of *polymerase chain reaction* (PCR) technology. The results of analysis of the DNA produced by PCR are much simpler to interpret and present in court.

As a practitioner, there is never the time to fully analyse or collate the information needed to properly answer questions which have bearing on the weight of significant issues. If forensic science is to fulfil its potential, there is a need to marry the superb technology available—opening up access to more and more sophisticated data—with the ability to make sense of it in reports and in court.

The future is challenging. It will require leadership and commitment and the willingness to risk failure.

References

Shapiro, H.T. 1990, 'The willingness to risk failure', *Science*, Editorial, vol. 250, no. 4981, p. 609.

Lloyd 1991, 'Talking Point', *New Scientist*, 21 September, pp. 1–2.

COMPUTER IDENTIFICATION SYSTEM (CIDS): HISTORY, SYNOPSIS AND FUTURE DIRECTIONS

David Chadwick
Director
C & R Technology Pty Ltd
South Australia

History

SINCE THE FORMATION OF THE MODERN DAY POLICE FORCES BY SIR ROBERT Peel, investigators have had the problem of identifying suspected persons. Unless the offender was known to the victim or had left their fingerprints at the scene of the crime, police had to rely on either descriptions circulated to the public by posters or through the media, or on likenesses drawn by the police artist.

In 1968, Jacques Penry presented his *photo-fit* system to the Home Office in London. His system consisted of photographs of police officers which had been cut into five facial components, namely eyes, noses, mouths, chins and hairstyles. These photographs could then be assembled together to form a likeness of a wanted person. This innovative system was quickly adopted by the majority of police forces throughout the world but, owing to a copyright dispute in the USA, it has not been updated since the mid–1970s. This has created the problem of outdated hairstyles and accessories, such as beehive hairstyles and bowler hats. In addition, the Penry system suffered from different skin densities which resulted in mosaic style of images with dark and light features joined by visible straight lines.

In 1987, David Chadwick and David Russell were police officers stationed within the Technical Services Division of the South Australian Police Department. Through their liaison with members of the Crime Drafting Unit—the unit responsible for the construction of Penry images—Chadwick and Russell became aware of the limitations of the *photo-fit* system. As both men were avid computer users, they turned their attention to the problem and developed a prototype package to replace the Penry

photo-fit with a computer-based system. This package was named the Computer Identification System (CIDS) and was demonstrated to senior police officers. With Departmental support, and by incorporating the requirements of the Crime Drafting Unit members, Chadwick and Russell developed the system into a working package, which was formally adopted by the South Australia Police Department in March 1988, totally replacing the Penry system.

Originally developed on the Commodore Amiga 2000 computer, inherent problems made the developers look to other manufacturers for an alternative operating system. It was finally decided that the Apple Macintosh II series of computers represented the best balance between processing power and cost effectiveness. With the support and assistance of Apple Australia, the system has now been adopted by Western Australia and the Australian Federal Police in Canberra.

Synopsis

CIDS is a system—based on the Apple Macintosh range of personal computers—which is designed to allow police officers and victims or witnesses of crimes to construct a life-like image of a suspect's face on screen and then to produce a printed or photographic likeness of that image.

The system is based around a database of photographic quality black and white images in 256 shades of grey. These images are digitised into the computer, after the original photographs have been prepared via a patented process, exclusive to C & R Technology. This process ensures that density of the skin tones is equalised throughout the entire database. This enables the operator to assemble a face that is free of the differing skin tones and straight line portions that are the trademarks of the current Penry system.

It is the quality and integrity of this database that is the key to the success of CIDS and, as such, users of the system are not permitted to add additional facial features to the databases. All new features are created by C & R Technology or their agents and are then distributed to registered users. The photographs, once digitised into the computer, are then electronically 'cut' into five component facial features, namely: eyes, nose, mouth, chin and hairstyle. These features are then categorised according to facial attributes and placed into the appropriate section of the database. Different databases exist for each sex and ethnic group, however, the features from each database are interchangeable; for example, a female hairstyle could be used for a male image or vice versa.

Once prepared into a database form, the images are assembled into a facial likeness via an appropriate proprietary software package. At this time, Studio 8 (by Electronic Arts) is used. However, this package is subject to change as advances in technology and programming occur. (It should be noted that any software changes made will still be fully compatible with existing databases.)

During the construction of the face, any of the features can be manipulated in any number of ways, including stretching, compressing, bending and rotation, thus allowing the operator the freedom to construct the image to suit the description given by the witness/victim. The method of facial construction is completely freehand, with the features being assembled in the position and order required and not being locked into a grid.

When the facial likeness is completed, the operator can then add text to the screen if required and output the final image to a number of devices, including:

- polaroid or 35 mm film;

- postscript laser printer;
- dot matrix printer;
- video tape; or
- other CIDS computers, if networked.

Colour versus black and white

Research conducted by David Russell as a result of an overseas study tour has revealed that authorities such as the Federal Bureau of Investigation, Washington (USA), the Royal Canadian Mounted Police, Ottawa (Canada) and the Home Office, London (United Kingdom), all agree that a witness' interpretation of an offender's skin colour, complexion or hair colour are likely to degrade, rather than enhance the overall facial construction. As one can imagine, the variety of skin colours in Caucasians presents enormous problems for the witness in attempting to relate that one shade of flesh tone that is correct from the 16.7 million available through Apple Macintosh. This problem is magnified one thousand fold when attempting to describe skin tones of persons from other countries such as the Asia-Pacific regions or Africa.

It was realised on the information from these overseas law enforcement agencies that a description used as an adjunct to the constructed image enables the public to form their own interpretation of the offenders facial characteristics. This description would include items such as hair colour (for example, dark brown, sandy or blonde) or skin colour (ruddy, clean-shaven, pock-marked). To add these features to the image constructed on the computer would interfere with the overall impression of the offender.

It is most important to remember that these images are reconstructions from a person's memory usually formed at a time of extreme duress or trauma and, as such, are subject to outside influences in their accuracy. The whole purpose of construction of a facial likeness is to jog the memories of members of the public or assist in recognition of the pictured individual as someone they know.

The realm of facial construction utilising computers should be viewed as an adjunct to normal investigative procedures, along with fingerprints and physical evidence collected from the scene of a crime.

Future Directions

During the development of CIDS, Chadwick and Russell became aware of another problem in identifying suspects. The problem exists when an officer needs to conduct a photographic identification parade using a criminal photograph of the suspect in conjunction with eleven other, similar, photographs.

It has been found that the current failure rate for criminal photographs, taken when a person is arrested for an offence, is approximately 50 per cent. This accounts for an unacceptably high wastage of film and other resources and means that the range of photographs available for an officer to view are severely reduced. Also, in most police departments, there is a considerable delay in searching for suitable photographs with which to conduct the identification parade and getting the selected photographs printed. It has been noted that, in some cases, the delay can be as long as two days.

In observing these problems, C & R Technology are devising a total package to replace the current criminal photograph system. This package, called the Whole Image Retrieval System (WIRS), will comprise the following features:

- foolproof video systems within the police charging stations that will capture ten seconds of colour video of the arrested person. Research shows that the failure rate will be reduced to less than 1 per cent.
- data entry suites where operators will capture the video images onto computer and enter required details of the person. To safeguard the innocent, these images will not be accessible to users until a conviction is recorded.
- viewing suites where officers can call up individual images or search for similar looking images which can then be assembled into a photographic identification sheet on-screen. This sheet can then be printed on a photographic quality printer.
- estimated time for an identification sheet to be produced is fifteen minutes, with a greatly reduced consumables cost. In addition, the storage of bulky negatives is eliminated.
- the system will also use the categorisation methods of CIDS to enable operators to search for possible matches once a CIDS image has been completed.

In 1993, WIRS is now available in numerous configurations to suit Apple Macintosh and IBM compatible systems.

Further Information

Further information on the Computer Identification System (CIDS) or the Whole Image Retrieval System (WIRS), can be obtained from:

C & R Technology Pty Ltd
PO Box 518
BLACKWOOD SA 5051

Telephone: (08) 370 2830
Fax: (08) 278 8384

MICROPHOTOMETRY AND MICROSPECTROPHOTOMETRY

Dermot Allen
Leica Instruments Pty Limited
New South Wales

Microspectrophotometry

THE SPECIFICATIONS AND TECHNIQUES LISTED UNDER THIS SECTION ARE related to the Leitz MPV-SP microspectrophotometer system in conjunction with the Leitz Aristomet research microscope.

Microphotometry and microspectrophotometry is the technique of measuring light from a specific area of a microscope image. Measurements can be made using a variety of illumination techniques:

- Transmitted light: Transmissions and absorption measurements can be made to determine the amount of light transmitted and the amount of light absorbed by the specimen;

- Reflectivity: How reflective is the sample? This requires calibration against a reflectivity standard so that an absolute percentage of reflectivity can be measured. For this technique, co-axial incident light is required;

- Remission: This is a measure of reflected light but requires an oblique incident light source; and

- Fluorescence.

Measurement of the light intensity using these illumination techniques can be grouped into two main categories.

- Relative intensity between two or more specimens: This intensity can possibly be related back to a standard, as in the case of reflectivity measurements. To assist in the accuracy of light intensity measurements, it is normal to incorporate an interference filter between the specimen and photometer so that all measurements are done in monochromatic light.

- Spectral measurements: Here intensity is measured at a variety of wavelengths, most typically over the visible spectrum. This technique is referred to as microspectrophotometry. To achieve spectral measurements, a requirement is a device to split the light from the specimen into its component wavelengths. A diffraction grating monochromator is utilised for this. Exit slits between monochromator and the photomultiplier allow us to change the sensitivity with a choice of 6, 3, 2 or 1 nanometer half band widths.

Spectral measurements can be made using all of the illumination techniques mentioned earlier.

Specific Applications of Microspectrophotometry

Fibres

Spectral transmission and absorption of light passing through fibres using transmitted light is an important means of identification. For calibration purposes, a spectral intensity measurement is taken of an empty area of the slide adjacent to the fibre to be measured. This gives the 'instrument curve' and represents the maximum intensity achievable at all wavelengths as seen by the photo multiplier. Therefore, any wavelength that is presented from the sample at the same intensity as the standard (empty slide) will give a 100 per cent transmission. Variations in transmission versus wavelength will show as a graph with 1000 points from 0 per cent to 100 per cent.

Inks and paints

Measurements using oblique incident illumination are referred to as Remission measurements. For true colours to be seen of paint flakes, documents and similar items, incident illumination technique is important. Incident illumination techniques can be categorised as co-axial incident light techniques (Brightfield) and oblique incident illumination (Darkfield). Co-axial illumination only gives reflectivity information and will not give colour information.

A good example of this would be a document with lamination. Co-axial light will give reflection from the top of the laminate, thereby reflecting all wavelengths evenly and not imparting a colour. Oblique incident illumination, however, will show colour through the laminate. This technique essentially is exactly the same as transmission measurements mentioned earlier. As the mode of illumination is from above, an empty field cannot act as a calibration, therefore a 'white' standard is necessary which could be a white powder of Barium sulfate, aluminium oxide or a special white paper.

Fluorescence

The fluorescence spectrum of any specimen exhibiting fluorescence can be achieved using *Epi* fluorescence. This technique developed by Leitz uses filters to select excitation wavelengths of light to reach the specimen, the fluorescence caused is then observed.

Once a spectrum has been measured, many functions can be performed to investigate the characteristics of the spectrum further. These include:

- Smoothing: smoothing of graph to reduce noise. Smoothing interval and number of smoothing functions performed are optional;

- Derivation: this plots the Derivation of the spectrum and helps to show hidden peaks;

- Difference: subtracts one spectrum from another; and

- Colorimetry: this menu option allow colorimetric evaluation to DIN 5033. The data read out is in chromaticity coordinates x y z, tristimulus values XYZ. L*a*b and the LCH values for the standard illuminants A, C and D65 each for 2° or 10° standard observer. Graphics option shows the chromaticity coordinates x y in the CIE colour chart for the 2° standard observer.

Stored spectra can be compared using a spectral search program. This program produces a list of the top twenty closest matches as held in memory showing their percentage match. This is a powerful tool for comparing unknown spectra with a library of materials which have previously had their spectra analysed.

Any part of the spectra can be viewed in fine detail by changing the scaling of the graph. Spectra can be produced on paper by plotter or printer. Plotters have the advantage of colour to make comparisons easier. Data, graphics and numeric data can also all be printed out.

PHYSICAL DAMAGE TO TEXTILES

Nigel Johnson
Department of Textile Technology
School of Fibre Science and Technology
University of New South Wales

ANY MATERIAL COMPOSED OF FIBRES IS A TEXTILE, AND THIS DEFINITION covers an extremely wide range of products in everyday use. Worldwide, over 35 million tonnes of textile fibre is consumed annually, ending up not only as clothing, upholstery, bed linen and carpets, but also in such items as ropes, seat belts, nets, road stabilisation mats, drainage pipes and tents. It is not surprising that, when a crime takes place, the ubiquitous textile is nearly always present and is very often directly involved.

The successful use of textiles in such a broad range of applications is due in part to the great variety of fibres and fabric constructions that are available. Most textile items are compound structures composed of up to four levels—fibre, yarn, fabric and the final article—and within each level, there are many choices available. There are more than fifty types of textile fibre in commercial use of various lengths and diameters; for example, cotton, wool, flax, jute, nylon, polyester, acrylic and polypropylene. Normally, these fibres are formed into yarns of various types (for example, monofilament or multifilament; ring, rotor or air-jet spun; single, plied or cabled), and then the yarns are interlaced into fabrics, either by weaving, knitting, braiding or even knotting (in the case of nets).

In addition to the great many woven and knitted constructions, so-called 'non-woven' fabrics may also be formed directly from fibres, without the intermediate yarn form. Furthermore, while paper and leather are usually not considered as textiles, they are nonetheless fibrous structures, and the same damage analysis techniques can be applied to them.

It is this very variety which often makes textiles such an important element in forensic investigations (such as in matching of evidence), yet it also makes it difficult to devise a 'recipe book' approach to the interpretation

of physical damage. While fibre identification can usually be performed by a technician with general laboratory skills, the analysis of textile damage is usually left to a textile expert.

Physical Damage

There are various forms of physical damage which may be found on textiles; for example, 'normal wear-and-tear' resulting from normal use of textiles. This usually takes the form of a thinning of the fabric prior to a hole forming, but seams may also come undone, threads can catch and be pulled out from the fabric, or the fabric may even be torn. It must also be remembered that the fabric will probably have been cut in order to make the textile item. In forensic investigations, these forms of 'normal' physical damage must be distinguished from other forms which may be related to the crime.

In a violent scuffle, a fabric may be torn, and the seams often fail; the structure of the fabric may also be distorted. Fabrics may be neatly cut, either with scissors or by slicing with a knife. They may also be punctured by relatively sharp (for example, a screwdriver) or blunt (for example, a hammer) objects, and the nature of the damage will depend on the supporting material (if any) beneath the fabric. Note that the stabbing action of a knife may have features of both puncturing and cutting.

Pure tensile failure may occur, especially in ropes and webbing (such as seat belts and slings), although this can often be precipitated by some other form of damage which has weakened the textile.

Abrasive damage, normally considered to be due to 'normal wear and tear', can also be of forensic importance. For instance, a seat belt may fail to protect a passenger in an automobile accident if it has been previously caught in the door and allowed to drag along the road. Damage may also be inflicted by insects, such as moths and carpet beetles, which bite the fibre and digest the fibre pieces internally. Micro-organisms, such as some forms of bacteria and fungi, can inject enzymes onto the fibre to break it down.

There are many chemicals which can weaken, modify or completely dissolve some textile fibres. The exact nature of the damage depends on the chemical structure of the fibre and the local conditions, such as temperature and presence of other agents such as oxygen. Textiles may also be damaged by excessive heat, for example in fires or ovens. Heat damage could be localised if inflicted by a cigarette or blow-torch.

Thus, when examining a damaged textile item, the textile technologist is usually confronted by a wide range of possible general causes. This range must first be narrowed before any particular scenario can be evaluated.

Only physical damage caused by mechanical means which has led to a hole (or more generally 'severance', implying the breakage of yarns or fibres in the fabric structure) will be considered in detail in this paper.

Examination Techniques

Most of the information that can assist in determining the cause of some severance lies in the physical 'morphology' of the fibres, yarns and fabric at and near the severed edge of fabric. Information on this morphology is obtained by observation at varying levels of magnification, ranging from direct viewing by eye without magnification, up to the use of a scanning electron microscope with magnifications up to 10,000X. The majority of inspections are done using the optical stereo microscope at magnifications between 20X to 100X. The following general features are examined.

At the fabric level

- Distortion of fabric surrounding the severance, such as buckling or folds out of the fabric plane or tight threads.

- Changes to the normal thread spacing, including runs in knitted fabrics.

- Direction of the severance line relative to the thread directions in the fabric; for example, tears usually propagate parallel to one of the thread directions.

- The relative positions of the severed yarn ends. In cuts, the yarn ends usually line up quite well, whereas a puncturing action may rupture neighbouring yarns at different positions.

At the yarn level

- Relative positions of fibre ends within each yarn. A clean cut made on untensioned fabric will leave all the fibre ends ending in the same plane. This has been referred to as a *planar array*. On the other hand, tearing will cause the fibres to break at different positions along the yarn, leaving a less well-ordered yarn end. High tension may also cause the yarn ends to untwist when the yarn is broken, leaving a frayed appearance.

- Short segments of yarn may be created, especially by cutting actions. For example, in knitted fabric, 'loop snippets' are created if the fabric is cut at an angle to the thread directions.

At the fibre level

The ends of fibres may also show some characteristic features. Thermoplastic fibres develop *mushroom ends* if they fail in a high energy tensile failure due to localised melting, whereas most low energy tensile failures produce fibre end morphologies which depend on the morphological structure of the fibres. Some insects leave characteristic bite marks.

The end morphologies of fibres cut individually can reveal quite a lot about the implement which made the cut. Scanning electron microscopy is needed to clearly examine the fibre ends at the required magnification and depth of field. Scissors usually flatten the fibre end and give a somewhat roof-shaped end, while sharp knives may even leave tool marks characteristic of the particular blade. However, the situation is not so clear when many fibres are cut simultaneously, as occurs when a fabric is cut, since the fibres may crush each other under the pressure of the implement. Relatively few fibres may have been subject to the pure action of the implement, and it must also be remembered that there usually are many fibre ends already in the yarn, which may have been created by one of a number of processes in manufacturing. Consequently, there is some disagreement about the value of fibre end morphologies in some forensic work.

Other

Contaminants may help or hinder the investigation. Heavy contamination with body fluids can make the yarn end morphologies difficult to see, but can often give a clue as to whether a severance occurred before or after exposure to the contaminating fluids. Liquid contaminants also tend to bind the ruptured fibre ends together, restricting any tendency to fray. Some contaminants and debris can give clues as to the cause of damage. For instance, moth eggs would suggest searching for further evidence of attack by moth larvae.

Where multiple layers of fabric may have been damaged, a comparison of the damage features in the various fabrics can be very informative, especially if they are of different fabric types.

Simulation

Because of the great variety of possibilities, the forensic textile technologist frequently tries to reproduce the damage in a controlled simulation experiment. Care must be taken to reproduce as many of the known variables as accurately as possible. The test fabric should be the same as or very similar to the crime scene fabric (in fibre, yarn and fabric characteristics). Since the mounting and supporting of the fabric can have a major influence on the damage morphology, these aspects of the test conditions must also closely simulate the proposed scenario.

Stabbed Fabrics

Stabbing accounted for 26.7 per cent of the homicide cases which passed through the Sydney Coroner's Courts from 1982 to 1986 (Bonney 1987). Generally, interpretation of the stab wound is left to pathologists, but this is only possible if there is a body, and if the body is in reasonable condition. Consequently, textile technologists are usually only called in when the body is badly decomposed or missing altogether, but in many cases there would be merit in examining both the wound in the body and the damage to the garment.

The morphology of stabbed fabrics has been investigated by Heuse (1982), Monohan (1975), and Stacy (1989), with a view to being able to identify the general shape of a knife which might have caused a particular severance. These workers used simulation experiments with either pork flesh or synthetic skin to simulate the support given to the fabric by the human body. Heuse (1982) suggested that four different actions can occur as a knife penetrates a fabric:

- pushing: moves yarns out of the plane of the fabric, or relative to each other within the fabric plane;
- cutting: due to sharp transverse pressure on the fibres;
- shearing: due to blunt transverse pressure on the fibres; and
- tearing: caused by the fibres being extended to break.

As the point of a knife engages the fabric, it will either push into a yarn or between neighbouring yarns. In either case, it will eventually start to push the fabric into the body beneath, tensioning the fibres and yarns and either tearing or cutting them. The cutting edge may then slice through yarns in its path until a reasonably long cut is produced.

The blunter the tip of the knife, the more the fabric distorts before the yarns sever, and the more the yarns will fray because of the tension developed in them. This distortion due to the initial penetration, found at only one end of the severance for smooth single-blade knives, is useful for deducing that the cut was produced by a stab, the likely orientation of the knife (and hence where the assailant was standing in relation to the victim) and the sharpness of the knife tip. Very sharply-pointed knives do not produce this distortion. A number of general points from these investigations are summarised below:

The tip

In general, the blunter the point of the knife, the more difficult it is to make the initial penetration of the fabric. Consequently, the blunter the point, the more the fabric distortion around the penetration point, due to pushing of the threads, and the more the broken yarns in this region will fray because they fail under tension rather than by being cut.

The blade

The sharpness of the blade affects the shape of the severance. A sharp blade will neatly cut the yarns as it travels through the fabric, with little or no fabric distortion, whereas a blunt blade will tend to pull the yarns before eventually cutting them, resulting in distortion along the sides of the severance and increased fraying of the severed yarn ends.

Blade irregularities

The presence of scallops on a blade will increase fraying and distortion, as each scallop point strikes undamaged yarns at a high angle, pushing them out of the plane of the fabric in the same way as the penetration of a blunt blade tip. Imperfections such as notches have a similar effect, and may even 'pull' single threads in some fabrics.

Blade dimensions

The thickness of the blade influences the width of the severance, as the broken yarn ends are pushed apart by the passage of the blade. Consequently, single-edged blades with a thick, blunt back edge produce a tapered severance, because the blunt back pushes yarns away from the severance near the point of initial penetration. However, the yarn ends may spring back to varying degrees after the blade has been removed.

The width of the blade influences the length of the severance; however, this is also affected by the depth of penetration and whether there is any 'slashing' (movement of the knife parallel to the fabric plane) in the stabbing action. The tendency to slash is determined largely by the resistance offered by the support below the fabric. Because of the likelihood of slashing, the width of the knife should be determined from the shortest severance, although this may underestimate the knife width if the knife only partially penetrated the fabric.

Stabbing angle

The severances are usually straight unless the blade is tilted at an angle to its direction of motion. This may occur if the knife is held at an angle in the stabbing action, if it bends or deviates under the force of impact, or if the fabric is moving laterally to the knife. In these cases, various forms of curved or multi-directional severances are produced.

Secondary cuts

In many cases, the knife may draw the fabric into the wound, causing a fold. The fabric can be cut at the fold, giving a small additional cut in line with the main severance.

Fabric effects

The same knife can produce different severance morphologies depending on the type of fabric that is penetrated. For example, a denser fabric like denim is harder to penetrate than an open structure like lace. This is another reason why it is not possible to fully characterise fabric severance morphologies; it is necessary to examine the effect of a particular knife on fabric identical to that involved in the investigation.

While these descriptions may appear quite clear, there are so many variables in most situations that great care must be exercised in drawing conclusions about the cause of a severance. In many cases, it is necessary to proceed by eliminating possibilities, bearing in mind that similar morphologies can be created by different means.

Handling Damaged Textiles

It is important for crime scene investigators to know how to collect and handle damaged textiles that may require forensic examination. Since handling can alter the relative positions of fibres, it is useful to record the shape of the severance and its relation to the body, photographically if possible, *before* disturbing the fabric.

Great care should be exercised when removing any implement from the fabric and in removing the fabric from its environment, so as not to disturb the fibres or threads in the vicinity of the damage. The area should be inspected and any loose fibre or thread fragments collected and recorded. This applies also to any implements suspected of having caused the damage.

The fabric should be handled very gently and folded carefully to avoid distortion to the damaged region, preferably with the damaged area left flat and folded inside other layers of the fabric.

Any subsequent damage that may occur must be recorded. For example, if the severance is propagated by tearing during removal of the fabric from the scene, then this must be recorded, as the torn region could otherwise confuse the investigation. The taking of samples from the fabric, such as for blood analysis, must also be recorded to save the textile technologist having to identify cuts made by the pathologist's scalpel or scissors.

Washing the fabric will effectively destroy the evidence. The mechanical action rearranges the yarn positions and frays the severed yarn ends, so any removal of contaminant should be left to the textile examiner.

Summary

Both textiles and the damage which can be occasioned to them are many and varied. Nonetheless, armed with a knowledge of textile properties and a stereo microscope, the textile technologist is often able to gain insight into likely causes of the damage by studying the morphology of the damaged material. However, as a general rule, possible causes can be eliminated with greater certainty than they can be confirmed.

References

Bonney, R. 1987, *Homicide II*, New South Wales Bureau of Crime Statistics and Research, Sydney.

Heuse, O. 1982, 'Damage to Clothing Caused by Stabbing Tools', *Archiv fuer Kriminologie*, vol. 170, pp. 129–45.

Monohan, D.L. 1975, Damage to Clothing—Cuts and Tears, MSc Thesis, Strathclyde University.

Stacy, A. 1989, The Severance Morphology of Stabbed Fabrics, BSc Honours Thesis, University of New South Wales.

MAPPING: TYING DATA TO THE REAL WORLD

David Lewis
Manager Marketing and Product Development
Peripheral Systems Pty Ltd
New South Wales

NEARLY EVERYONE HAS, AT SOME TIME IN THEIR LIFE, NEEDED THE SERVICES of a police officer. When commencing the studies needed to produce this paper and to show the relevance of the Geographic Information System (GIS) to policing, it was necessary to establish what the bounds or purposes were for the maintenance of police forces. This paper will discuss the ways in which GIS may assist in the execution of policing duties.

The easily identifiable roles of policing are those of protecting life, preventing crime, enforcing the law of the land, keeping peace and harmony in society, safeguarding property, control of (and in a democratic society such as Australia, the maintenance of) freedom of movement of people from one place to another. The ways in which these objectives might be accomplished are somewhat more complex to identify. For example, to allow the roles of policing to be achieved, police forces must increase the feeling of community well-being and security, be more responsive to the needs of the community, encourage and assist citizens to share some of the workload in policing by way of Neighbourhood Watch programs and, in this age of financial restraint, be economical.

The police force of any state or nation requires instant access to data collected by various government and private agencies for the purpose of assisting the community, under the guidelines highlighted above. The data that is collected nearly always involves the entering or referencing of a geographic identity. Therefore, it is important that police have computer technology which has the ability to quickly analyse great volumes of data and visually display that data in a geographically meaningful way.

MapInfo is the GIS system used as a model in this paper and it is distributed by MAPINFO Australia—Peripheral Systems Pty Ltd. *MapInfo* was initially designed for the personal computer and now includes the

following platforms: Windows©, Apple Macintosh© and Unix© for both Hewlett Packard© and Sun Microsystems©.

GIS and Spatial Analysis.

The term *spatial* refers to the identification of the space surrounds of a particular entity, and maps are very effective drawings of the spatial relationships of physical objects, one to another. The collected data referred to in this paper contains a geographic identity, and in most databases there is usually a field or series of fields into which data related to addresses is loaded. It is this series of fields that this paper will elaborate on.

Geographical data most often consists of three fields: a single entry for street number, name and type, another for suburb, and another for postcode. Each of these items becomes a geographic entity in relation to the other; that is, the street details can exist within the boundaries of either the suburb field or the postcode field. However it is possible to ask for street details and not stipulate any qualifier. The computer will then do a simple database search and display all requested street details encompassed by many suburbs and postcodes. For example, assuming the street detail given to the computer is '256 Pacific Highway', the Pacific Highway in Sydney travels through many suburbs, and in each suburb the numbering of that roadway begins again, therefore it is possible to have several listings for '256 Pacific Highway'. This need not be the only way that a geographic entity may exist. If police units have established boundaries relevant to their investigations, then the street details may then be qualified by a special boundary segment, thus making it unique to all other street details.

The way in which *MapInfo* works with street details is to assign the location to equidistant points between segments known to contain the appropriate range of street number addresses within a defined boundary, whatever that polygon represents.

The key forces in GIS today are those that argue the earth science role of GIS—software for the development of answers to the global questions of human survival on planet Earth. But just as the global situation can be assessed and a course of action recommended, so too can a police patrol, district or region be shown and activity of varying types overlaid on a specific geographic.

The premise that the presence of more data will lead to better analysis and, therefore, a better understanding of a situation is dangerous because of the lack of 'increased-load' handling methods. Police officers are, like all people, capable of data overload[1]. The level of understanding may vary and, consequently, the level of perceived information by any police officer will vary.

The time lag between collection of data and reaction to the information derived from that data is a concern. Examples include the Three Mile Accident in the USA, or Chernobyl in the former USSR—both situations were

[1] The term 'data overload' is used because, until that data is processed and is understood by the recipient, it is not information.

severely hampered by a lack of clear information. In situations such as these, geographic information systems are crucial.

GIS and Layers of Data

Layering of data can be thought of as the use of plastic overlays on a traditional street map. An overlay may graphically denote a boundary of either police investigation or patrol, the size of the boundary being determined by current needs. Another plastic overlay may graphically denote a particular street path to be followed, while yet another overlay may be added which indicates points of relevant data. When these overlays or layers are shown together, they present a picture which is more easily understood than the same data presented in text form. It is little wonder that the saying *a picture paints a thousand words* has such support in these circumstances.

The application of layering to a normal policing environment involves adapting stored data that is already available. An example in the case of investigation of robberies, would be the use of a detailed map that has symbols to indicate the properties that have been robbed. These symbols could be coloured in different shades, highlighting the type of robbery that took place. Immediately a pattern can be seen, whether the properties were usually residential or commercial premises, or whether a certain type of robbery method was used.

An advantage of a GIS is that complex and unusual layers of data can easily be overlayed on the details already displayed. For example, a list of known persons whose method of operation matches that under investigation and their last known places of abode can be displayed. Again the symbol and the colour could be different. The known methods of operation could even be mixed to give a possible connection between previously unrelated matters.

The basal geographic data that is capable of being displayed can vary according to need and layers of data related to streets, suburbs, towns, railway lines, stations, parks, forests, fire trails, rivers, lakes and even private access roads can be described. Over this data, boundaries peculiar to police needs can be superimposed to show regions, districts, patrols, sectors and beats in the normal organisational running of a police force. Other layers could include Neighbourhood Watch programs and Safety House zones. These can then be easily seen to fall within particular police control areas and officers then can be more rapidly assigned or organised to work within those locations.

The work of search and rescue or siege situations can be more comprehensively controlled with the use of a GIS. A comprehensive map can be made available to the control team which shows not only the roadways and other standard GIS data, but also utility companies already using GIS can make their data available; for example, water mains, stormwater drains, mines and subsidence areas, mine shafts, canals, access points and directions of flow of these structures.

Once all these data are layered onto the patrol or beat map familiar to the police officer, a new perspective may suddenly appear; for example, the

likelihood of either a search being fruitful in a given area, or the possibility of capturing an escapee.

Other Uses of a GIS

Together with the more glamorous uses of a GIS, products such as *MapInfo* can be used in day-to-day police operations for organisational aspects such as identifying locations of police officers on the move. An officer can radio their position to a central control area which can then update the computer map with that location. Should there be a need for an urgent response, all units' locations are known and the most appropriate unit can be despatched to the call. GIS can also be of assistance in monitoring patrols; for example, if, for some reason, a unit does not report at an appropriate time, a nearby unit can be diverted to investigate. The GIS method is more efficient than a manual system because a trace can then be created (if the system is established this way) to more accurately model the actions that took place leading to an arrest or the prevention of crime (this is known as modelling).

Modelling using a computer system to map out the action that took place is already in use in Victoria where a CAD (computer-aided drawing) package is used to record a case and graphically represent a chart of how a crime was committed. A CAD package such as AutoCAD provides drawings that can be loaded into a GIS such as MapInfo, thereby giving the best of two worlds. The use of CAD in the courtroom is estimated to save the Victorian police $30,000 a day.

MapInfo also has the facility to perform mobile tracking of objects or individuals through satellite transmission. A history of movement could be constructed to substantiate claims made by police in their surveillance of suspects. Already there is a company whose vehicles are equipped with this technology thus enabling them to monitor and ensure the safety of the company's product.

The advantages that mobile tracking could provide to policing strategies include those responsible for traffic management being able to decide on least-cost traffic routing, time to next destination (very important in emergency situations), and vehicle positioning both for the safety of officers and the community. Even the satellite duress alarm identification may be useful. *MapInfo* can concurrently track many individual units and show the location of an object to within fifty metres on the mapfile datasets provided. This type of central control would be paramount in an organisation the size of most police forces.

Another activity that a GIS can perform specific to policing needs is the ability to display police data on a map screen and perform *what-ifs* with that data. This is much like using a spreadsheet, and investigations to project the possibility of certain events occurring can be carried out. Similar geographic investigation can be done for disaster relief work. Through mathematically projecting the rise of water using a GIS, *what-ifs* can be performed to determine which streets and houses will be first affected by rising flood waters. Occupants of homes near a river or storm-water drain will obviously

be evacuated first, should the need arise. The functionality of the GIS is that software can do projections for situations that have yet not been experienced by people; for example, predictions for a once-in-one-hundred-years flood can be made without having to rely on guesswork and memory.

Conclusion

There are many uses for a system that is designed to relate spatial data visually, and the GIS can be effectively used by a wide variety of people. But perhaps, as mentioned earlier, to be able to manage a force of people whose occupation requires them to be out in the community they serve, there is not any greater need than to see.

COMPUTERISED FACIAL CONSTRUCTION AND RECONSTRUCTION

Adrian Paterson
Detective Sergeant in Charge
Criminal Identification Squad
Victoria Police

FACES ARE FASCINATING. THE COMBINATION OF FIVE BASIC FACIAL FEATURES can create millions of variations. From the time when mankind began to draw on cave walls, artists have endeavoured to produce what the eye perceives in hard-copy. Along with the infinite naturally-occurring facial variations, human error in the form of individual perceptiveness widens the degree of inaccuracy in portraying the likeness of a subject.

Whether one is endeavouring to identify criminal suspects, unidentified deceased or missing persons, what must always be remembered is that it is impractical to assume that 100 per cent accuracy can be attained. With the advent of computers, the basic processes involved in depicting facial images have altered very little, but the applied science of computer graphics has meant that these processes can now be extended far beyond what could have been envisioned years ago.

As the leading Police Artist Unit in the world, the Victoria Police Criminal Identification Squad (CIS) in Australia has, since 1986, developed a full-colour Facial Automated Composition and Editing system known as FACE. There were a variety of similar systems on offer from private overseas companies, all of which offered what was thought the police should have. The CIS, as police forensic artists, designed a system that would do what our forensic artists wanted it to do. As a result, the CIS entered a new world with more versatility than had ever been envisaged.

FACE Details

FACE is a personal computer-based system with one main workstation linked to two additional workstations on a token ring network. Each workstation can be used to interview victims and witnesses and has its own personal computer, high-resolution colour graphics monitor and a graphics tablet. The two smaller workstations access the main database (as does the main unit), where hundreds of facial components are

stored on a 600Mb hard drive. The database is full-colour and comprises both male and female Caucasian, Aboriginal, Asian, Southern European and juvenile components.

Each component database is further broken down into sub-menus; for example, eyes that are open, medium, and closed; and mouths that are thin, medium, and full. A user-friendly menu allows the police artist to display each component in either a grid of sixteen per page, or to scroll through each category with the witness[1] able to see each component in relation to the others on-screen. Once the hair/forehead is chosen, the chins can then be scrolled through until one is selected. This chin component can then be moved up or down to arrive at the closest overall face shape. In turn—or in order of the witness' most vivid recollection—the eyes, noses and mouths are displayed until a full face has been assembled.

At this stage, accessories such as spectacles, moustaches, and beards can be displayed separately and, once the chosen feature has been nominated, the original face image reappears on the screen and the selected accessory is automatically displayed in its correct position on the image. If, for some reason, the skin tone of one facial component is darker than the others, the menu provides for a *fix* function which identifies the average skin colouring of the whole face and automatically adjusts the skin tone of the nominated component, matching all closely. An automatic blending function then smooths out the joins between each facial component, leaving a completed image of almost photographic quality. During their training, investigators are taught to accept these life-like images, not as photographic references, but as computer-generated images of varying accuracy as dictated at the end of each victim or witness on a scale of 1 to 10.

To this stage, the FACE system could be operated by a person with little or no computer knowledge and thus achieve results far better than any other system available in the world.

If the services of a police forensic artist are available, then the next step is to exit from the main menu into the world of colour graphics and an artistic software package which enables extensive enhancements to be made to the original image. These enhancements can include:

- manually restyling the hair or changing it dramatically, even reducing it to bald;
- changing the nose from the bridge to the tip; for example, broadening or breaking it;
- changing the eye colour and shape, including the eyebrows;
- altering the mouth in any way;

[1] The term witness as used in this paper will incorporate the victim.

- reshaping the chin, adding facial hair or suggesting an unshaven shadow; and

- adding wrinkles, scars or any other blemishes.

Any changes sought by the witness can be complied with, resulting in an image in which the accuracy is restricted only to the memory and recall of the witness. Images are then stored in colour, and data relating to the complainant, offence, offender and investigating member is added to complete the interview. The image is printed out in full colour and immediately handed, with the data, to the investigator.

Any image can be digitised into the FACE system to enable any user to input his or her own photographs and to break the face down into the respective sub-databases for later recall. In this way, any FACE user can create their own database of desired features and nationalities.

A portable version of the FACE system complete with database, video-still camera, graphics capabilities and full-colour printer is mounted in a van and used by the CIS as a mobile interview unit. It can attend at crime scenes or country divisions and provide a complete identification service to the whole state of Victoria.

Facial Recognition

It is important at this stage to highlight the fact that a computer can do no more than it is directed to by a human being. Even the combination of the forensic artist's artistic ability and the FACE system's versatility will produce no better image than that which can be described by the witness.

In an effort to fulfil the role of forensic artists, the CIS are duty-bound to expand investigative endeavours to the point where there is nothing further that can be done to improve the image attained and to ensure that the witness has also exhausted their recollection of the subject. If a witness described a suspect as having green spiked hair with a solitary yellow eye in the back of his/her head, the forensic artist should be able to produce an image which accurately depicts that suspect. It is not the role of the forensic artist to question the beliefs of the witness or to enter into any form of disagreement with them regarding any comments or statements made which may conflict with the investigator's personal understanding of the events.

The one rule to be remembered is that witnesses have seen someone that the investigator has not. Witnesses have some idea, and the investigator has no idea of what the suspect looks like. Therefore, whatever a witness tells the artist is more than is presently known.

What is important, however, are any influencing factors which may reflect on the ability of the witness to recall the suspect accurately. These include the following:

- time lapsed between incident and the interview;

- degree of physical trauma involved (passive to violent);

- whether the person was a victim or a witness;
- day-time/night-time—lighting conditions;
- distance from offender;
- use of weapons by offender;
- use of disguises by offender;
- duration of commission of offence;
- period offender observed;
- witness observation capabilities;
- witness' ability to retain the image;
- witness' ability to recall and describe;
- the age or demeanour of the witness;
- the willingness of the witness to cooperate;
- whether the offender was seen on more than one occasion; and
- whether the offender is known (by sight) to the witness.

It is a matter of course for the forensic artist to be naturally aware of these factors in assessing the evidentiary value of the witness.

The Victoria Police CIS interviewed in excess of 2,600 witnesses during 1990–91. Of these, a great proportion were able to direct and assist the artist in completing a computer-generated image of the offender. The remainder fell into a group who invariably were unable to recall individual facial features, but would know the offender again if they saw him/her.

In the past, these witnesses would be shown numerous photographs of offenders and asked to select individual facial components. The chosen features would then be hand-sketched into one single image—known as a *composite drawing*. Although composite drawing enjoyed some success as an alternative identification technique, it was little more than a stopgap effort to obtain a description where *Identikit* and *Photo-fit* failed.

Using the FACE system, the composite drawing exercise can be taken infinitely further. Not only can the chosen photographic components be digitised into FACE within moments, but the components can also be blended together into one colour image. Prior to FACE (when the process was hand-sketched) the witness could, when they saw the completed composite image, comment that they thought a feature looked similar to the offender's when seen in the original face, but when the feature was repositioned into the composite, it did not look right. It is now possible to vary the chosen feature by stretching, reshaping or artistically altering it using the flexible

computer software drawing capabilities. If necessary, the selected components (which in their reassembled form appear acceptable) can be retained as displayed on the screen. A wide selection of features can then be superimposed within that image and scrolled through to enable the victim to see the variables on offer actually changing the face in front of them.

On some occasions a witness may select only one photograph and comment that this face was not the offender, but that is quite similar to him/her. Suggestions are then made by the offender to alter the face and these requests can be complied with as the witness watches the changes take place. Ultimately, the image may become further removed from the chosen original yet becomes a very close likeness to the offender.

There is another type of witness who (for whatever reason) is able to positively identify the offender and will 'never forget the offender's face as long as he/she lives'. This witness is, of course, invariably better than others. Very few witnesses leave the CIS offices without providing a description of the offender or suspect.

Witness/Artist Interaction

A great deal has been written about witness identification. The reliability, accuracy and relevant evidentiary value of eye witnesses has been dragged under the microscope and torn apart by theorists and observers who conduct laboratory-controlled experiments and hypothetical exercises to establish whether or not the human brain's neurones are capable of analysing and processing information in either a collective or individual form.

However, police have to deal with human frailty, emotions, individuals and circumstances, each incident being far removed from the last. The only person who fully understands the importance of bonding with the witness on this common ground is the forensic artist, who interviews as many as 250 witnesses per month, sits for hours alongside a rape victim, and tenderly extracts details while watching for emotive changes. The forensic artist is always careful not to breach the fine line of suggestive involvement, while suppressing the investigative urge that grows within any police forensic artist.

It is also important for the artist to be a police officer, for the depth of witness interaction can become greater with the help and understanding sought by victims in their time of need. Witnesses will relax and open up more to those with whom they feel comfortable and secure, as compared with an outsider who is brought in to assist in the case. A striking example of this was the reaction of a ten-year-old girl who was the victim of a disgusting abduction and sexual assault. On completion of the interview with the police officer/artist, she embraced the officer, hugged him tight and thanked him for helping her. The descriptions obtained from the child, such as, offender facial features, vehicle, weapons and other related items, resulted in the identification and subsequent arrest of the offender. The human bond and professional understanding is immeasurable in obtaining good results in these situations.

Colour

Much has been written on the value of using colour when obtaining descriptions, yet it has been claimed that colour is not an important issue. This is not so. Not only is colour important to the witness, it is also to the investigator.

Whether or not the completed image is as correct as police would wish it to be, the availability of colour is deemed to be essential when obtaining a description of an offender. With *Photo-fit*, a forehead may be selected as being similar, with the hair a very similar style to the offender, but the hair is a dark tone and the offender was blond. Ideally there should be a blond, medium and dark version of the same hairstyle, but this would effectively triple the size of the *Photo-fit* component base and still not provide the ability to alter the hair length and other features (except for the Chinagraph pencil).

The FACE system stores and displays in colour, and it is this capability which enables the artist to gain more from the witness. If colour enhances witness recall—which it does—and produces a more accurate image, then it must be incorporated in the identification process.

As detailed by Davies & Ellis (1978), the *Identikit* composites in a study by Laughery & Fessler (1971) were not communicating all the information witnesses had available to them. A further study by Ellis, Davies & Shepherd (1978) and Laughery, Fowler & Rhodes (n.d.) suggested that the 'feature by feature' approach (for example, perusing pages of eyes and noses as individual features in catalogues) as used by *Photo-fit* and *Identikit* was less successful than by working with groups of features.

As *Identikit* was the only facial construction tool available between 1960 and 1970 and *Photo-fit* from 1970 onwards, the FACE system was created with thirty-three operational requirements as the development criteria. The main need was for the witness to be able to view the face image as a whole and to be able to assess the overall image. If necessary, the witness was to be able to either scroll through and change the nose or mouth if it did not look right or, alternatively, widen the forehead or narrow the bridge of the nose.

A witness who has initially expressed reservations regarding their ability to recall an offender's description has ultimately surprised themselves by progressive refinement (Laughery, Fowler & Rhodes n.d.). Note, that in this study, Laughery refers to witnesses working with a sketch artist.

The forensic artists of the Victoria Police CIS have achieved the unique ability to combine the best of both these systems, with a full-colour photographic-quality database which is capable of being artistically changed at the will and direction of the witness to produce the most accurate and detailed description possible for use by investigators.

Computer Ageing

As a result of the marriage between forensic artist and computer, the Victoria Police CIS began to extend the squad's capabilities and services. In 1990 the Victoria Police Missing Persons Bureau (MPB) requested the CIS to assist in the ageing of missing schoolgirl, Eloise Worledge. It had been ten years since she went missing and the MPB were endeavouring to regenerate public attention and awareness. Using a combination of artistic ability and computer versatility, Eloise was aged from ten to twenty years.

This was the first step down an unknown path for the CIS and, as well as artistic interpretation and professional knowledge, the study of facial growth and development was also undertaken and is continuing in conjunction with members from the Melbourne University and the Royal Melbourne Institute of Technology (RMIT).

It is not known what a person will look like in ten or fifteen years' time. Will an individual put on weight or lose weight? Will they accumulate numerous facial wrinkles or 'bags' under the eyes? What about baldness or greying? No-one knows and neither does a computer. The area of computer ageing is venturing into an unknown world where speculation prevails. What can be done, however, is to minimise the variables and endeavour to work within accepted growth guidelines, using these guidelines not as a 'rule of thumb', but as an indication of the changes one would reasonably expect to develop during the natural ageing process.

It is known that in the early years of life, the cranial cavity (which dominates the top two-thirds of the head) consolidates, losing the protective fluids in a progressive pattern of growth development. The face, previously one-third of the head size, lengthens and narrows and the resulting downward movement of the nose and mouth is seen as the jaw begins to set.

Very extensive computations have been carried out in overseas endeavours to achieve the ultimate computer ageing results. These results are generalised and still only predict a likely change in the appearance of the subject once applied. The exercise of projecting extensive growth patterns and measurements into a computer and then programming the computer to make the suggested changes is queried. Surely, once the growth patterns and measurements are known, the forensic artist can move the chin down to the required length, broaden the base of the nose, extend the ears and narrow the face using his own ability. Existing computer-programmed systems require an experienced medical illustrator or artist to make these appropriate modifications or alterations and, by using an additional software program, cosmetic enhancements such as hairstyles are added.

This is little more than the CIS are presently achieving using manual artistic ability. Australia is fortunate that it does not have the high incidence of reported missing children as is experienced overseas. But despite the volume of subjects, the ageing processes remains the same. However, the CIS (in conjunction with John Glover of RMIT and Vision Control Australia) are working towards the development of a simplified personal computer-based growth guide program. This will finetune present ageing techniques and provide accurate relative growth/age reference points from which CIS artists can rebuild the face.

By accepting that certain facial dimensions remain static with young children, the face begins to develop its own individual facial characteristics. Between the eyes, the bridge of the nose becomes established, as the length and shape take form due to cartilage development. As teeth grow and the second set of teeth become set, the jaw is forced to accommodate them and adjust accordingly to provide proportional jaw movement and bite. As a result, the chin lengthens further and, in doing so, proportionally draws the lower facial features down with it, slightly affecting the cheeks as well. Eyes and brows do not change dramatically but the mouth fills out with teeth development, generally affecting the lower lip more than the top. Once again these are general rules and the resulting images can in no way be deemed to be an accurate update.

In adult life, changes are more subtle. The lines of age and those that develop from actions such as habitually frowning establish one as an individual. Apart from distinctive facial characteristics, it is often the facial lines that give a person (or FACE image) the added extra definition which makes it that much more distinctive from another. Changing hairlines and the build-up of fatty tissue also ensures additional individualism.

The practical application of ageing techniques when applied to adult subjects has evolved from requests to update or age a photo of an offender where the only photo is, perhaps, ten years old. If investigators intend undertaking a search for this person, they bring the photo to the CIS where a forensic artist will apply ageing techniques, using the FACE computer's versatility and their artistic ability, to generate an updated likeness. This is then printed out in colour and handed to the investigator.

Facial Reconstruction of Unidentified Deceased Persons

Taking this technology a step further, the CIS has been working closely with Dr John Clements of the Department of Odontology, Melbourne University, and Ron Taylor, Advanced Maxillo Facial Technician, of the Peter McCallum Hospital in Melbourne in the facial reconstruction of unidentified deceased persons. To explain the process of facial reconstruction, this paper will refer to one of the first such joint undertakings.

The request for facial reconstruction was initiated following the findings of a skull in north-western Victoria. Other skeletal remains and a fragment of clothing was all that remained of the body which had been burnt. The tip of a hunting arrow was found in the skull, deemed to be that of a Caucasian male. At the request of the Melbourne Homicide Squad, Ron Taylor embarked on the laborious task of measuring and assessing, using the International Table of Soft Tissue depth, by locating eighteen bony landmarks on the skull. Once the pegs were in position, the muscles are placed in their correct position of origin and insertion. The skull is searched for any irregularities in the mandible before being completed. Once this process is finalised, the resulting reconstruction is in the form of a three-dimensional white plaster bust.

The next step in the facial reconstruction was to photograph and digitise the image into the FACE system and to position the image within the parameters of the existing component database. If there was any evidence of hair colour and texture, hairstyles are searched for a similar match and then superimposed onto the image. The skin colour is then added and the two blended together. Lips are coloured and pupils, lashes and brows drawn onto the image displayed on the graphics screen. The once white bust has now taken on a more lifelike appearance.

What must be remembered is that this image, although considerably enhanced, still retains unknown characteristics such as eye detail, nose peculiarities, ear shape and specific hairstyle. This process has, however, taken cranio-reconstruction further down the identification path than previously enjoyed.

Reconstruction of Traumatised Deceased

There are occasions where unidentified victims of homicide, suicide or suspicious death are not suitable for media release. There are also occasions where identification of a deceased person is impeded by the severity of the injuries inflicted.

The CIS (using the FACE system) has begun directing their artistic abilities towards the reconstruction of traumatised deceased. Once again, it must be remembered that the computer cannot produce better results than it is directed to do.

Sceptics have questioned the value of computer involvement in the world of art, yet fail to understand that computers serve only to extend and enhance an artist's ability. Computers do not take the place of the artist. This is never more evident than when applied to forensic investigations.

A basic application of reconstruction relates to the death of an adult male in Victoria in October 1991. A passerby noticed a hangman's noose swinging from an inner-suburban bridge which spanned the Yarra River. On returning a short time later and seeing the rope still there, the passerby climbed onto the bridge, retrieved the rope and conveyed it to the nearest Police Station. Forensic tests on residue speedily ascertained that the residues on the rope were in fact human. Divers searched the Yarra River, which flows into Port Phillip Bay several kilometres downstream. The search failed to find a body, but did retrieve a head. It had been severed at the neck, apparently due to the combination of the distance of the drop, the weight of the body and the diameter of the cord used. Previously there was no quick, practical way by which the head alone could be given media exposure in an effort to identify the deceased.

The CIS, using a Canon ION Video Still Camera, took a number of colour images of the head from various angles. These images were electronically transferred onto the FACE system and a three-quarter face and side profile were selected for further work. Firstly, the three-quarter image, with the eyes half-closed and the bottom lip torn through with tongue exposed, was displayed. In turn, the eyes were slid sideways and enlarged. Working with a full-colour palette, each eye was then enhanced, eyelids opened, pupils restored (with highlights added to give life to the image) and details refined before the eye was reduced and placed back into the correct facial position. The mouth was corrected next. By selecting colours from the face itself (straight off the screen), the torn mouth area was repaired, blended and reinserted back onto the face. Finally, the hair was tidied and an open-neck shirt was drawn onto the neck area where torn flesh was previously obvious. All of these embellishments took no longer than fifteen minutes and the result was printed out in hard copy and full colour, in time for media release to television stations. A short time after the image went to air, police received a call from a viewer who recognised the deceased and enabled official identification to be achieved.

The same computer graphic process is applied to each reconstruction, only with varying degrees of complexity.

A second case study resulted from the discovery of a young woman's body which was found lying on the floor of an abandoned warehouse. She had been murdered only days before and the same side of her face that received multiple blows was also the side suffering the effects of post-mortem lividity. As in the previous case, photos of the deceased were digitised into the FACE system and the CIS artist set about reconstructing the face of the deceased. With one-half of the face in reasonable condition, the facial features were sufficiently distinguishable to clean and enhance the nose and cheek areas by selecting various skin tones and 'spraying' the colours onto the face gradually restoring the complexion.

The eyes were opened and enhanced, the hair restored to a style similar to that already evident and the mouth gradually tidied and recoloured. The whole face was then smoothed, blended and given a final touch-up. This resulted in a traumatised face being restored with considerable accuracy suitable for media exposure and subsequent identification.

A recent request for CIS assistance came from the Montreal Police Force in Canada. In a drug-related murder, the deceased in question suffered horrendous injuries, which included multiple stab wounds to the face with the eyes being pierced, ears severed, nose sliced through and severe soft-tissue damage to the entire face area. The extent of the injuries was such that the request was almost refused but, after extensive study of the numerous colour photographs, X-rays, pathology reports and other relevant details, the same reconstruction processes were applied. The existing nose portion was 'mirrored' to provide the basic nose shape and length. One eye, although recessed into the eye socket, was sufficiently distinguishable as to size and colour to enable it to be enhanced, repositioned and (as with the nose) mirrored over to provide the second eye. One eyebrow was also retrievable and repositioned. The mouth area proved the most difficult to reconstruct and would have been the least accurate component of the face. The overall facial shape was acceptable and the hair required minimal attention. X-rays were invaluable in assessing the bone structure which showed a prominent brow and full upper teeth and jaw, filling out the top lip more than the lower. The resulting image portrayed a male aged in his thirties. But, although appearing to be a miracle in facial reconstruction, the face was not deemed to have been restored to its former appearance. The degree of facial trauma was so extensive that speculative interpretation and artistic licence was used to provide a suggested appearance of the deceased and it intended to serve as a guide or indication to the victim's possible identity.

Conclusion

There is still much to learn and understand in the field of facial identification, but with a team of dedicated forensic artists and the best equipment available, facial construction and reconstruction forms the foundation from which forensic artists can build and expand on professional offerings to investigative officers in the field.

References

Davies, G.M. & Ellis, H.D. 1978, 'Face Recognition Accuracy as a Function of Mode of Representation', *Journal of Applied Psychology*, vol. 63, pp. 180–87.

Ellis, H.D., Davies, G.M. & Shepherd, J.W. 1978, 'Remembering Pictures of Real and Unreal Faces: some practical and theoretical considerations', *British Journal of Psychology*, vol. 69, no. 4, November, pp. 467–74.

Laughery, K.R. & Fessler, P.K. 1971, *Human Memory and the Identification Process*, State University of New York, Buffalo NY.

Laughery, K.R., Fowler, R.H. & Rhodes, B.T. (n.d.), *Factors Affecting Facial Recognition*, Mug File Project Report No. UHMUG–3, University of Houston, Houston TX.

VIDEO RECORDING OF EVIDENCE: THE 'I CARE' PROJECT

John Heslop*
Inspector
North West Region Command
New South Wales Police Service

FROM THE OUTSET, IT MUST MADE BE CLEAR WHAT THE TERM 'VIDEOTAPED evidence' means when used in this paper. Videotaped evidence is that evidence captured and recorded on videotape. For some reason, closed circuit television (as used in the Australian Capital Territory and New South Wales courts) and videotaping have become one. In fact, this paper refers to a victim—a child—giving evidence on closed circuit television which is then shown on a court television monitor in a courtroom. This paper will describe the 'I CARE' project and the place video technology plays in that project.

Background

Some three years ago, the author was appointed the coordinator of the Child Protection Program in the New South Wales Police Service. Part of the duties of the coordinator was to look at research with a view to improving police investigations of allegations of child abuse, and specifically child sexual abuse. Videotaped interviews involving child victims of sexual assault, police officers and social workers are not new. In fact, in the 1985 New South Wales Child Sexual Assault Task Force Report (New South Wales 1985), one of the recommendations advocated videotaping child victims' evidence.

The winds of change have blown somewhat slowly and at times in the wrong direction, but in New South Wales, those winds have finally blown the correction direction. The time is now right to look carefully at the procedure of videotaped

evidence. The task of research into the use of videotaped evidence was made somewhat easier when a travelling research fellowship under the auspice of the Australia-Britain Society and a research grant under the auspice of the New South Wales Police Service were awarded. Those grants allowed the author to observe child abuse investigation procedures and related technology in the UK, Germany, Canada and the USA.

United Kingdom

In the UK, time was spent with the London Metropolitan Police and the Greater Manchester Police. Both organisations have dedicated child protection teams who jointly interview child victims with social workers. All teams interview on video or audio tape.

An interesting aspect to interviewing on videotape is that, in 1991, there is still no legislation in England that specifically addresses videotaped evidence. However, in 1989 the British Government established an advisory group on videotaped evidence under the chair of Justice Thomas Pigot (Great Britain 1989). The Pigot Report, as the *Report of the Advisory Group on Video Evidence* has become known, has since been released and the recommendations are still being deliberated upon by the British Government, so radical are its recommendations.

Not deterred by the lack of legislation or adoption of the *Pigot Report* recommendations, the child protection teams in London and Greater Manchester still interview child victims of sexual assault on video or audio tape. These tapes can still be introduced into evidence, but not as the evidence of the child victim.

Canada

In 1989 the Canadian Federal Bill C–15—which specifically addresses child abuse and supplements the Criminal Code of Canada—was introduced. In Canada, the Metropolitan Toronto Police and the Ontario Provincial Police were observed at close quarters. In both police services, the use of video technology in the interviewing of child victims of sexual assault is used.

United States of America

In the USA, similar observations were made at the Seattle Police Department in Washington State and the Orange County Police in California. It is interesting to note that a large number of states in the USA have enacted legislation which permits videotaping in child abuse cases. It is also a fact, however, that a number of the states have repealed the legislation due to bad experiences or because of the underutilisation of the video technology.

Does underutilisation of technology mean it is not effective? Yet, Scandinavian countries routinely use video technology and experience no difficulty in having the tapes admitted into evidence.

The Australian Position

It is understood that in South Australia, video captured evidence from child sexual assault victims can be admitted into evidence as long as transcripts of the tapes are available to the court. In Queensland, there is specific legislation which allows video captured evidence from child victims of sexual abuse to be admitted into evidence and children are also interviewed on videotape in Victoria.

In New South Wales, Section 3 of the *Children (Care and Protection) Act 1987*, states:

> regulations made under the Act, may regulate the recording by audio/video tape, of interviews with children concerning a personal assault.

However, such recordings are not admissible into evidence, except when subpoenaed by the defence as evidence of a prior inconsistent statement. In other words, the audio or video recording can only be used to discredit a child witness rather than to support them. This is an outrageous piece of legislation, to say the least. Thus, there is no statutory authority to videotape evidence given by child victims of sexual assault in New South Wales.

During the author's research fellowship overseas, the New South Wales Attorney-General had written to the Minister for Police and Emergency Services requesting that a pilot program be developed whereby child victims of sexual abuse could be interviewed on videotape. This program would fall in line with the new procedures where police in New South Wales interview specific suspects on videotape. Accordingly, the author was asked to establish an interdepartmental working party in December 1990.

This Working Party consisted of representatives from the Police Service, the then Department of Family and Community Services, the Health Department, Office of the Director of Public Prosecutions and the Attorney-General's Department. It was decided by the Working Party that a twelve-month pilot program would be established to trial the new procedure.

Aims of the New South Wales Program

The pilot program was named 'I CARE' (Interviewing Children And Recording Evidence). The Working Party developed the following aims for the I CARE program:

- rebut claims of contamination of evidence in child sexual assault cases;
- elicit sufficient information from the child to document the alleged abuse;
- increase professional credibility and competence of police and Department of Community Services' officers;

- improve the quality of statements taken from child victims in child sexual assault cases by improving interview skills;
- seek to minimise further trauma to the child during the interview process;
- conduct the interview in a manner that will aid the investigator and will permit legal proceedings to be taken where appropriate;
- obtain information required for an effective case plan to be formulated; and
- facilitate an increased understanding and improve working relationships between the Police Service and the Department of Community Services.

The Pilot Program

Newcastle was chosen as the I CARE pilot area due to close working relationships between Child Mistreatment Unit investigators and the officers from the Department of Community Services and also because of the availability of a purpose-built video interviewing facility at the Community Health Centre at Wallsend Hospital. This facility, used ordinarily for family therapy, has an interview room separated from the control room by a one-way mirror. The building in which it is housed is apart from the main hospital and is available 24–hours a day, seven days a week. A large number of children attend the health centre on any day and, as such, it was thought that this would make the facility more attractive for use when interviewing child victims.

It was decided that an equal number of officers from both agencies would be involved in the pilot program. Nominally, all available officers from the Child Mistreatment Unit would be used. It was proposed that an officer from the Police Service and a local Community Services officer would interview jointly.

The Working Party also had to develop a protocol for use by the project members prior to, during and after the interviews. Issues covered in the protocol are:

- what happens when a disclosure is made to police or Department of Community Services officers;
- consent to interviews;
- criteria for interviewing victims;
- how the equipment operates;
- the number of copies of tapes that are made;

- sequence to be followed from time of disclosure to completion of interview;
- rapport building;
- interviewing sequence;
- ending the interview; and
- procedures for worker debriefs.

Equipment

As this Conference is a technology-orientated conference, perhaps this would be an opportune time to briefly explain the hardware used in the I CARE project.

Technology developed by SVT Video Systems Pty Ltd (Sydney) was used for the Electronic Recording of Interviews with Suspected Persons (ERISP) Project. As the developmental work had been done for the ERISP project, it was thought to be worthwhile to 'piggy-back' on their technology which could be easily adapted for the I CARE project.

The preferred recording system was a combined video and audio recording system. These 'hybrid' recorders produce three master audio recordings on compact cassettes together with two video recordings on the VHS format. The I CARE system differs from the suspect interview system in that it has a remote camera, multiple remote microphones and a small remote control panel. When a child is interviewed, two video and three audio tapes are produced. A master video and audio tape are secured away, the second videotape and an audio tape are used by the investigating team, and the third audio tape is sent for transcription.

Training

An integral part of the I CARE pilot project was the training of interviewing officers. Queensland Police embarked down this road in 1989–90, eighteen months prior to I CARE and, as already stated, Queensland has legislation which supports this move. Through the New South Wales Police Commissioner, an approach was made to the two training officers in the Queensland Police Juvenile Aid Bureau to assist with training.

The Queensland course had been developed to suit Queensland Police procedures, legislation and technology. It therefore followed that some modification to the Queensland course content was required. To this end, the two Queensland trainers, two New South Wales Police Academy trainers in child abuse investigation and the author modified some sections of the course to suit the I CARE pilot program.

In February 1991 an intensive one-week residential training course was conducted. In total, eighteen participants took part in the training program. Topics such as communication, interviewing, and videotaping skills, childhood development, legislation, and legal and equipment issues were covered in the course. Whilst there were mixed feelings at the commencement of the course, evaluation comments at the completion of the course showed that all participants found it to be more than worthwhile and essential to success of the project.

The I CARE Project

Formally, the I CARE project was launched on 4 March 1991 at Newcastle. Since then, a number of child victims have been interviewed, the youngest being three years old.

Conclusion

This paper illustrates the I CARE project and its development. It is now obvious that the concept of videotaped interviews with child victims of sexual abuse is supported. Yet, what are the advantages of using such technology in an area such as child sexual abuse investigation?

- it has been shown to reduce the number of interviews;
- it encourages *Pleas of Guilty*. This is confirmed in Victoria, the UK and certainly in Minneapolis in the USA, where in the first year of using the technology, sixty out seventy-five offenders pleaded guilty;
- it is the best possible evidence, that is, the victim can be seen and heard, and that is not available in written statements;
- it assists in persuading disbelieving family members;
- it is easier and quicker for the interviewer;
- it reduces confusion and stress on the child; and
- it assists the relevant agencies charged with preparing the case.

Looking at the other side of the coin, only two disadvantages can be seen and both have no impact on the child:

- if the interviewer is not skilled in relation to interviewing and the type of questions to be asked, the use of video technology becomes a wasted effort; and
- by having a videotaped interview, anyone can see and hear what was said and done, including gruesome and embarrassing details.

The I CARE project has had its share of teething problems and, in the equipment area, these have included:

- the difficulties in obtaining a balance between the need for visual coverage of the whole interviewing room and the need for clarity of facial expressions of the child being interviewed;
- excessive background noise on tapes;
- placement of microphones; and
- quality of videotapes used.

We are about to enter the twenty-first century. Technology and its advancement can help bring about better treatment of sexually abused children—surely they are owed that.

> The worth of a society can be judged by the way a society treats its children (Bronfenbrenner 1970, p. 63).

Acknowledgment

The Queensland Police Service must be thanked for letting the I CARE pilot project use their project name, as their project has been a success. It is hoped that Queensland's success might also rub-off onto the New South Wales project.

References

Bronfenbrenner, U. 1970, *Two Worlds of Childhood: US and USSR*, Russell Sage Foundation, New York.

Great Britain. Advisory Group on Video-Recorded Evidence 1989, *Report of the Advisory Group on Video Evidence* [The Pigot Report], Home Office, London.

New South Wales. Child Sexual Assault Task Force 1985, *Report of the New South Wales Child Sexual Assault Task Force*, Government Printer, Sydney.

PUTTING SOUTH AUSTRALIA ON THE MAP

Leanne Weber
Acting Manager
Special Projects Section
South Australia Police Department

FOR MOST OF THE POLICE PARTICIPANTS AT THIS CONFERENCE, THE MOST exciting advances in police technology have, no doubt, been those which assist in the detection and prosecution of offenders. However, alongside this trend towards a more sophisticated police response to crime, a shift of emphasis towards crime prevention must also be acknowledged. This shift has created its own pressure for more sophisticated information technology to assist in the planning and evaluation of crime prevention initiatives.

The Crime Mapping System was developed by the South Australia Police Department (SAPD) in response to this need, using funds from the South Australian Government's *Together Against Crime* strategy. As well as the obvious objective of representing the geographical distribution of crime in the state, the Crime Mapping System was designed to map selected census information so that crime patterns could be compared with socio-demographic patterns. Importantly, crime and census data was also to be combined before mapping so that standardised crime rates (for example, housebreaks per household or assaults per population) could be displayed in areas of relevance to both the police (for example, in administrative police divisions) and the public (for example, in local government areas).

Although detailed computerised information on the offence location and offender's residence had been collected by the SAPD for some time, reports at this level had never been readily available, and certainly not in the form of a map. The smallest units which can be represented in the maps are Census Collector Districts (CDs) which usually consist of around 300 households.

Thus, the potential for using maps to assist in the development of local, community-based crime prevention initiatives through the Together Against Crime strategy was realised from the outset. In fact, the Attorney-General's Department, which coordinates the Together Against Crime scheme in conjunction with local governments, has now been supplied with a copy of the Crime Mapping System and data so that they can provide project officers attached to Together Against Crime committees with crime and census maps under agreed policy guidelines. This

unprecedented data sharing has not been without teething problems, but the adoption of a cooperative approach suggests a new era of greater openness in the sharing of information between police, the community and other agencies. This is in keeping with the successful overseas approaches to community-based crime prevention, notably France, on which South Australia has modelled its approach.

Because of the early focus on community-based crime prevention, the Crime Mapping System met with a mixed response within the SAPD during its development. The SAPD's Crime Prevention Services section could see the advantages of visually representing crime statistics in local neighbourhoods for planning and monitoring their Neighbourhood Watch program. But outside that bastion of community policing, many officers could not see the benefits of a purely statistical system which had neither the timeliness nor the ability to pinpoint individual criminal events. The 'pinpointing' ability would, in their view, give the system 'operational' or 'tactical' relevance. Furthermore, with the added disadvantage of having only imagination to go on, many could not see how crime maps could offer anything new, since the maps depended mainly on information which was already available within the SAPD.

However, with the completion of the Crime Mapping System in April 1991 and the gradual extension of its use within the SAPD, many of these preconceptions are being overturned. Applications are being discovered for the system in a wide range of situations. Experimentation with the powerful data manipulating capabilities has demonstrated that new information may be derived from old, by combining and representing information in ways which were previously not possible or feasible. Finally, and most importantly, the increasing acceptance of proactive, information based approaches to policing has brought a noticeable change in the SAPD in the two years since the conception of the idea for the Crime Mapping System. This has meant that 'research' and 'planning' are no longer, at worst, dirty words or, at best, activities to be carried out by civilian specialists buried in the depths of police headquarters. Officers of all ranks will be increasingly expected to research and plan their own local initiatives, and this requires locally-based information which can be readily understood.

In early 1991, a training video to acquaint members of the SAPD with the capabilities of the Crime Mapping System and the relevance of crime and census maps to their work was developed. To do this five realistic police situations were devised to demonstrate both the technical features of the Crime Mapping System and the application of its outputs to a variety of policing problems. This paper is based on those five situations, since the objectives and target audience for which they were devised seem to correspond with the objectives and target audience of this conference.

For readers who would like more background information on how the Crime Mapping System was developed, please *see* the paper 'Mapping Crime in South Australia' in *National Overview on Crime Prevention* (Weber 1992).

Situation 1: Monitoring and Evaluating Neighbourhood Watch

The scene

A Neighbourhood Watch coordinator in Whyalla is struggling to prepare for an approaching meeting with residents. She does not know how she will be able to answer the barrage of questions they have been asking about how their neighbourhood compares with others; whether Neighbourhood Watch simply shifts housebreaks to areas without programs; or whether criminal activity shifts away from housebreaks to other targets, such as cars, in Neighbourhood Watch areas. She does not have the access to the data or the statistical expertise to investigate these issues in depth.

The maps

Maps can help to illuminate some of these issues in a way which non-statisticians can readily understand. Neighbourhood Watch areas (which correspond to two or three CDs) operating at a particular date can be indicated on the map by an 'N' or by printing the actual number which identifies a particular program. Comparisons can then be made readily between neighbourhoods with and without a Neighbourhood Watch program. (Note: the whole of Whyalla is now covered by Neighbourhood Watch.) A series of similar maps can be produced to monitor changes in patterns over time; for example, possible movements of offences from Neighbourhood Watch to non-Neighbourhood Watch areas as new programs start. The legends on the maps can be fixed so that a particular shading pattern has the same meaning in all maps[1] (by default, the value ranges are calculated automatically to suit the distribution of records in a particular map).

The outcome

Residents are better informed about crime in their area and the SAPD is better able to tailor programs, if necessary, to local needs.

Situation 2: Identifying Targets for Problem-Oriented Policing Strategies

The situation

A patrol team at the Para Hills Police Station has been involved in a trial of the Problem-Oriented Policing technique. This requires patrol officers to identify recurring problems which drain police resources and cause community concern, and then devise strategies for their resolution. The team has recognised the need to make physical changes to the carpark at a key public transport interchange to prevent motor vehicle thefts and interferences. They need to approach the local council and other relevant agencies to obtain approval and funding. For most of them this is a new challenge and they want to be as well prepared as possible.

[1] Crime maps are being used extensively in a comprehensive, state-wide evaluation of Neighbourhood Watch which is being conducted by specialist social science researchers in Special Projects Section.

The map

A map showing selected motor vehicle offences in the Para Hills Division illustrates dramatically the problem in the collector district which contains the interchange and a major shopping centre (shaded dark). Note that the blank areas may still have a considerable number of offences reported during the year, but individually they are insignificant in comparison with the solid shaded area (*see* Figure 1).

Figure 1

Motor Vehicle Theft and Illegal Use in the Para Hills Subdivision
1 January 1990–31 December 1990

Number Reported

Note: Counting rules applied. POLDIV–01.

The cross-hatched area has experienced considerable development since the boundaries were determined for the 1986 census and, therefore, contains far more households than other areas in the Division. This may account for the slightly elevated incidence of motor vehicle offences in this area. (Note: This problem is inherent and unavoidable with any CD driven system, including the census data itself.)

This particular map does not give Para Hills police information they did not already have, but it provides a persuasive tool for negotiation with the council. If desired, the map can be printed direct to transparency for presentation.

The outcome

The council and other agencies are easily convinced that resources should be allocated to this project. The interchange carpark now has a fence, neatly trimmed trees and a security guard.

Situation 3: Designing Offender Programs through the Together Against Crime scheme

The situation

Following a Together Against Crime public meeting, a group of local youth workers approaches the police with a proposal to increase facilities for young offenders in their area. The police offer to obtain crime maps to investigate the reported crime problems in their suburb relative to neighbouring suburbs.

The maps

The police realise that, for an offender-based program, it is more relevant to map the residence of apprehended offenders than the location of offences. They request a series of maps of their Division showing the number of offenders for various offence types in selected age groups in each CD. The youth workers are surprised to see that despite their perception of high youth crime and misbehaviour in their area (which may nevertheless be true), known criminal offenders are generally resident in neighbouring suburbs.

The outcome

The youth workers decide to change their approach to concentrate on after-school care exclusively for children who are resident in their area. They believe the approach they had originally intended may have had the unintended outcome of attracting young offenders from other areas into their own. Community resources are better allocated and police relations with other agencies have been enhanced through effective cooperation.

Situation 4: Developing a General Crime and Community Profile

The situation

A commissioned police officer has been assigned to a new suburban posting. The officer is keen to obtain a quick overview of the characteristics of the community in the area and the key crime indicators. The officer is also interested both in how this Division compares with others in the metropolitan area, and in the crime and socio-demographic patterns within this new Division.

The maps

An enormous range of crime and census maps could be of interest to the police officer. For example, a map showing the age structure of the population in this new Division will tell the officer at a glance whether this Division has a high or low population aged under eighteen years, when compared with other metropolitan Police Divisions. More detailed maps can be accessed which demonstrate the effects of standardising crime rates.

The outcome

A good overview of broad community characteristics and a better understanding of the true nature of crime (for example, by examining both absolute and standardised crime rates) gives the police officer a sound basis for planning.

Situation 5: Developing A Strategic Intelligence Assessment

The situation

An intelligence officer used to performing tactical intelligence tasks is asked to investigate emerging trends in, say, armed holdups (this could easily be offences such as credit card fraud, stranger rapes, or any number of issues of current interest). How does the intelligence officer start to investigate?

The maps

A map showing the current geographical distribution of the category of crime to be investigated can be a useful starting point. This can provide a conceptual framework to get a difficult project started. More detailed maps can then be produced for areas of particular interest, and changing patterns over time can be investigated.

Because of the facilities within the Crime Mapping System to calculate new data items and extract subsets of records before mapping, a series of highly specialised maps can then be produced to address specific questions; for example: Do different areas show different patterns of day time/night time offences? Do some areas have a higher proportion of one sub-category of offence (for example, a higher proportion of robberies which are armed robberies) than others? The possibilities are limited only by the detail available in the source data. Of course, many questions which arise will not be amenable to analysis using crime or census maps. Where geographical patterns are not of particular interest, conventional statistics and graphs are still far better tools. The answers to other questions may require information other than crime or census data. In this case, the Crime Mapping System may still be of some assistance since it has facilities for mapping external data, that is data collected from sources outside the SAPD.

The outcome

Maps can be tailored to test specific hypotheses being investigated by the intelligence officer by selecting subsets of records for mapping and calculating new customised data items.

Conclusion

Although developed initially for the information of community-based Together Against Crime committees, the Crime Mapping System is now finding a variety of applications within the South Australia Police Department. The usefulness of the system to operational police has been assured by its ability to represent data in geographical areas which are meaningful to both the police and the wider community; and its ability to manipulate and combine data in new ways which add to the understanding of crime and society.

Crime mapping is now taking its place among the arsenal of research and planning tools which will be required by police officers of all ranks in the approaching era of proactive, information-driven policing. An even greater challenge will be the increasing demands to share this information in a constructive and open partnership with the community.

Reference

Weber, L. 1992, 'Mapping Crime in South Australia' in *National Overview on Crime Prevention*, eds S. McKillop & J. Vernon, Conference Proceedings No. 15, Australian Institute of Criminology, Canberra, pp. 203–208.

NON-LETHAL INCAPACITATION

Robert Hamdorf
Chief Superintendent
Deputy Director
National Police Research Unit
Adelaide
South Australia

IN SIMPLE TERMS, NON-LETHAL (OR LESS-THAN-LETHAL) INCAPACITATION means 'to render a suspect incapable of action by means of force which is highly unlikely to cause death or serious injury when properly applied'. In America, this process requires that the suspect fall to the ground as a result of the force.

An important caveat at this point is to emphasise that it is unrealistic to expect that a non-lethal force option means that it will be 100 per cent less-than-lethal 100 per cent of the time. There has been considerable attention given to the use of various forms of non-lethal force in the USA and Canada brought about by, among other things, realisations by police administrations that the use of deadly force must be a last option, courts reviewing police use of force (including deadly force) making it clear that less-than-lethal options must be used before the last option of deadly force is considered, and growing public opinion against the use of force which inflicts serious injury or death.

In Australia, the National Committee on Violence recommended, among many other things, the following:

> *Recommendation 85*. All governments should recognise and support:
>
> *Recommendation 85.1* Uniform laws throughout Australia . . . which should reflect the principle that lethal force be used as a last resort . . .
>
> *Recommendation 85.2* The provision of adequate resources (including funding) to ensure police receive adequate training in the use of firearms and non-lethal weapons . . . non-violent restraint and conflict resolution strategies . . .

> *Recommendation 85.4* The provision of funding for the development and deployment of non-lethal incapacitating weapons . . . [which] should be evaluated, to ensure they minimise the risk of injury to bystanders, suspects, and police . . .
>
> *Recommendation 86.* All police administrators should . . .
>
> *Recommendation 86.2* Develop and implement a code of conduct for law enforcement personnel which specifies that personnel may use force only when strictly necessary and to the extent required for the performance of their duty . . .
>
> *Recommendation 86.6* Develop national minimum standards relating to the validation and accreditation of firearms training and use of other weapons, including non-lethal weapons (National Committee on Violence 1990, p. XLi–XLii).

Although the use of deadly force in Australia cannot be measured to the same extent as overseas, there is no doubt that the level of violent crime is increasing, heightening the probability of greater levels of force, or more effective forms of force, being required of police. As previously indicated, this trend is growing in combination with a growing demand from the public and parliaments for greater care in the exercise of force to ensure that only that which is necessary to do the job—and that which will minimise the likelihood of injury to bystanders, suspects and police—is used.

Recent research on the topic of non-lethal incapacitation has included a thesis report on non-lethal weapons presented by Sergeant Greg Meyer of the Los Angeles Police Department (1991) and a report from the British Columbia Police Commission (1990). These publications have provided a useful compilation of material on the subject of non-lethal incapacitation, particularly given the paucity of literature on non-lethal weapons.

Forms of Non-Lethal Force

The following examples are representative of non-lethal force options given that there are variations within each category.

Acceptable in varying degrees

- Verbal control/presence, such as tactical communications;
- karate kick;
- pain compliance;
- nunchaku;
- pressure points;
- punch;
- miscellaneous bodily force, such as choke holds, arm holds, and so on;

- flashlight;
- swarm, where several police attack from various directions;
- chemical irritant spray, including capsicum (capstun), tear gas (CS, CN) and mace;
- electronic stun devices, such as taser, ultron, and nova;
- the Arwen 37 rifle which fires rubber cylindrical batons, tear gas or stun grenades (for use by tactical operations groups only); and
- stunning explosives (again, for use by tactical operations groups only).

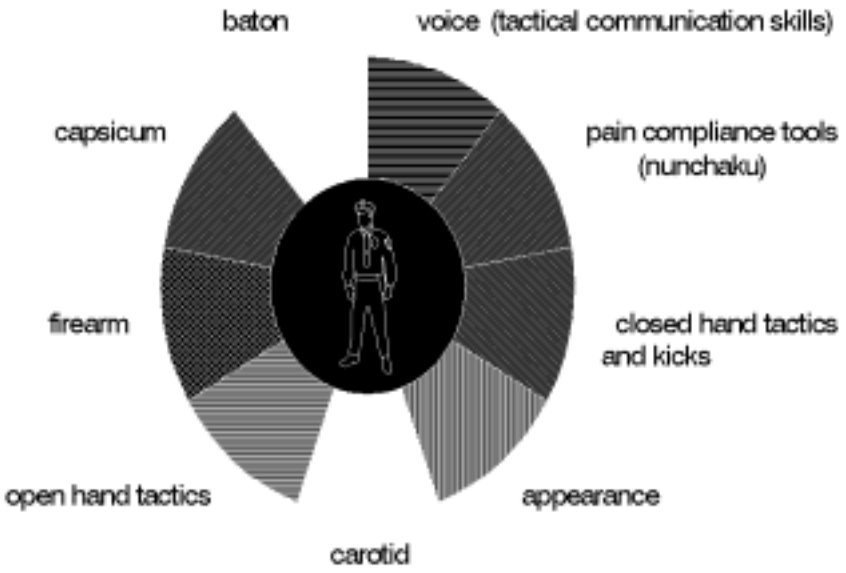
Unacceptable in Varying Degrees

- Come alongs (stick with noose);
- beanbag gun (deadly at close range);
- rubber bullets (deadly at close range);
- tranquillising guns (difficulty in judging correct dose; it is easy to over- or under-dose);
- electric shock device needing direct physical contact; and
- capture nets, leg grabbers, and the Immobiliser (combination of poles and chains). These take time to deploy, set up and apply. Once applied there is a strong probability of a fierce struggle when suspect is unwrapped, to enable the application of handcuffs.

Obviously, several of the non-lethal measures or weapons are already utilised to varying degrees by Australian law enforcement agencies. However, there is a reasonable risk of injury to police and suspects from the application of such measures. This is the single strongest reason for the pressure from courts, coroners, community pressure groups and governments for the search for and deployment of more sophisticated non-lethal (or less-than-lethal) weapons.

America and Canada have adopted a framework which emphasises the use of the least amount of force necessary to suit the particular circumstances—and this framework is one which has several available options of escalating levels of force available for officers to choose from. The *Situational Force Model* (*see* Figure 1) seems to be the acceptable format which can be modified to suit any agency's force-option policy. This concept replaced the 'incremental level of force' idea, which implied that an officer needed to work through from the least force level towards the greatest for every situation regardless of the inappropriateness of some force types.

Figure 1
Situational Force Model



The situational force model requires selection of the least violent means available, relative to the situation. The officer relies upon reasoned discretion in making the selection (Canada. British Columbia Police Commission 1990, Appendix B).

Although set in the Los Angeles Police Department (LAPD) environment, Meyer's 1991 research revealed some interesting statistics and outcomes. The LAPD has 8,000 members serving 3.5 million residents, in addition to which there are many thousands of commuters and tourists. They attend 863,000 routine, urgent and emergency calls plus thousands of officer-initiated contacts, 320,000 arrests and 750,000 traffic violations. Officers reported using non-deadly force to effect arrests on 3,602 occasions (ten per day) (Meyer 1991, p. 5). The LAPD police are trained to handle resistance by way of an increasing scale of force—such as verbalisation, firm grip, compliance holds, batons, karate kicks, chemical irritant sprays, Electronic Stun (Taser), upper body control holds, and then firearms.

When Meyer analysed the departmental reports required of each officer who used force against a suspect, he was able to determine the comparative levels of injury to suspects and police from the various force types, the types of incidents resulting in the use of the most frequently effective force type, and the success rate of each force type. (Note that the incidence of HIV/AIDS has caused many USA police departments to consider the heightened personal risk to officers using close contact control measures with suspects, particularly those using holds near the mouth.)

Table 1 outlines the injuries to suspects when the force used was effective (that is, made the suspect fall to the ground). It is interesting to note that Chemical Irritant

Spray and Taser resulted in no moderate or major injuries and only one minor injury, whereas the use of a baton resulted in seventy-three moderate or major injuries (60 per cent of baton incidents), and the use of a flashlight resulted in twenty moderate or major injuries (83 per cent of flashlight incidents).

Table 1

Injuries to Suspects by Effective Force Type*

Effective Force Type	*Suspect Injuries where Force Effective*					
	None	Taser/Gas	Minor	Moderate	Major	Total
Baton	24	0	24	66	7	121
	17.39	0.00	38.71	37.71	33.33	24.10
Kick	20	0	9	12	0	41
	14.49	0.00	14.52	6.86	0.00	8.17
Punch	6	0	5	15	1	27
	4.35	0.00	8.06	8.57	4.76	5.38
Miscellaneous Bodily Force	51	0	20	58	6	135
	36.96	0.00	32.26	33.14	28.57	26.89
Flashlight	4	0	0	14	6	24
	2.90	0.00	0.00	8.00	28.57	4.78
Swarm	33	0	3	10	1	47
	23.91	0.00	4.84	5.71	4.76	9.36
Chemical Irritant Spray	0	18	1	0	0	19
	0.00	16.98	1.61	0.00	0.00	3.78
Taser	0	88	0	0	0	88
	0.00	83.02	0.00	0.00	0.00	17.53
Total	138	106	62	175	21	502
	100.00	100.00	100.00	100.00	100.00	100.00

* Taser/Gas means effects of Taser or chemical irritant spray only.
Note: chi2 (28) = 589.5352 Prob>chi2 = 0.000

To compare, the injuries to police in the same incidents are outlined in Table 2. It is interesting to note that, once again, Chemical Irritant Spray and Taser resulted in no injuries to police and no effect from the tear gas/taser. This is not entirely supported in a later survey which showed only 14 per cent support for the tear gas because of the residual effects of the gas on police vehicle seats and prisoner clothing. The other types of force show significant injury levels.

Table 2

Injuries to Suspects by Effective Force Type*

Effective Force Type	*Suspect Injuries where Force Effective*					
	None	Taser/Gas	Minor	Moderate	Major	Total
Baton	99	0	4	10	8	121
	23.35	0.00	30.77	26.32	36.36	24.10
Kick	36	0	0	3	2	41
	8.49	0.00	0.00	7.89	9.09	8.17
Punch	19	0	0	5	3	27
	4.48	0.00	0.00	13.16	13.64	5.38
Miscellaneous Bodily Force	109	0	5	13	8	135
	24.71	0.00	38.46	34.21	36.36	26.89
Flashlight	20	0	3	1	0	24
	4.72	0.00	23.08	2.63	0.00	4.78
Swarm	39	0	1	6	1	47
	9.20	0.00	7.69	15.79	4.55	9.36
Chemical Irritant Spray	14	5	0	0	0	19
	3.30	100.00	0.00	0.00	0.00	3.78
Taser	88	0	0	0	0	88
	20.75	0.00	0.00	0.00	0.00	17.53
Total	424	5	13	38	22	502
	100.00	100.00	100.00	100.00	100.00	100.00

* Taser/Gas means effects of Taser or chemical irritant spray only.
Note: chi2(28) = 171.9286 Prob>chi2 = 0.000

Table 3 indicates the frequency of use of effective force types used to bring the incidents to conclusion. The most frequently observed were the baton, Taser (Electronic Stun) and miscellaneous bodily force (pushing, shoving, and tackling).

Table 3

Incident Precipitating Conditions by Most Frequently Observed Effective Force Types

Type and Number of Precipitating Conditions*		*Effective Force Type*					
		Most Observed		2nd Most Observed		3rd Most Observed	
PCP	(35)	TASER	(16)	Baton	(6)	Misc	(5)
Other Drug	(70)	Misc	(18)	Taser	(17)	Baton	(12)
Alcohol	(176)	Misc	(52)	Baton	(39)	Taser	(31)
Mental	(93)	Taser	(32)	Baton	(21)	Swarm	(17)
Footchase	(119)	Baton	(49)	Misc	(33)	Flashlight	(11)
Disorder	(201)	Misc	(49)	Taser	(48)	Baton	(41)
Domestic	(65)	Misc	(23)	Taser	(13)	Baton	(12)
Attack Officer	(193)	Baton	(61)	Misc	(48)	Taser	(25)
Attack Citizen	(61)	Baton	(17)	Misc	(16)	Taser	(14)
Other	(84)	Misc	(24)	Baton	(17)	Taser	(13)

* Conditions listed had at least thirty observations.

Having considered these statistics, it is worthwhile combining injury rates with corresponding success rates of force types (*see* Table 4). The success rates ranged from 75 per cent for the punch to 96 per cent for the flashlight. However, the injuries sustained question the real success. The punch had the highest combined major or moderate injury rate (36 per cent) for officers, while the flashlight had the highest rate for suspects (80 per cent). However, the Chemical Irritant (tear gas) and Electronic Stun (taser) had a zero per cent injury rate whilst their success rate was 90 per cent and 86 per cent respectively.

The British Columbia Police Commission (BCPC) approached the question from a different angle. Where the LAPD had been using non-lethal weapons for several years, the BCPC set out to select the most appropriate weapon. For various reasons the BCPC chose to select or promote the:

- side handled baton;
- capsicum spray (an organic extract of cayenne pepper which does not have the environmental residual and, therefore, decontamination problems);
- Orcutt police nunchakus (to be used principally as a pain compliant tool not a striking weapon); and
- Arwen 37 Rifle (for use by tactical teams).

The BCPC avoided the:

- electronic stun device due to the need for personal contact with suspects and, therefore, the risk of injury to police (this was not the same device as the Taser used by the LAPD);
- mace (which is a tear gas product) due to the effects of the residual left on clothing and the environment and the subsequent decontamination problems as described by many LAPD officers; and
- flashlight due to the fact that they can cause serious injury.

Specific instructions have been issued against use, and various other options for various negative reasons.

Table 4

Success Rates of Force Types, with Corresponding Injury Rates

Force Type	Study Cases*	Success Cases	Success Rate (%)	Major/Moderate Injury %~ Officers	Suspects
Baton	143	121	85	16	61
Kick	47	41	89	11	26
Punch	36	27	75	36	64
Miscellaneous	143	135	94	15	46
Flashlight	25	24	96	4	80
Swarm	51	47	92	16	24
Chemical Spray	21	19	90	0	0
Taser	102	88	86	0	0
Total	568	502	88	13	39

* Includes Effective and Ineffective Force Types.
~ Percentage of major and of moderate injuries, regardless of whether force was effective.

Conclusion

Apart from the adoption of a Situational Force Model approach to the application of force and a greater emphasis on the training in and use of tactical communications, there are no firm thoughts on which, if any, of the other non-lethal weapon options should be adopted by Australian law enforcement agencies. It is firmly believed that real efforts must now be made to identify or develop acceptable non-lethal (or less-than-lethal) weapons for use in Australia.

Of course, there is the matter of public acceptability—but then there is already a growing level of public opinion against some of the measures in use in 1991. It is

hoped, therefore, that this paper has provoked some logical thoughts for law enforcement agencies to consider, particularly in light of the National Committee on Violence recommendations and in preparation for the changing moods of the community in the future.

Acknowledgments

The author acknowledges, with thanks, the contributions of the British Columbia Police Commission and Sergeant Greg Meyer of the Los Angeles Police Department to this paper.

References

Canada. British Columbia Police Commission 1990, *Recommendations of the Committee on the use of Less Than Lethal Force by Police Officers in British Columbia*, British Columbia Police Commission, Victoria BC.

Meyer, G. 1991, Non-Lethal Weapons –v– Conventional Police Tactics—the Los Angeles Police Department Experience, thesis.

AN INTRODUCTION TO FIREARMS SIMULATION TECHNOLOGY

Eric Danielsen
Managing Director
Inwood (International) Pty Ltd
New South Wales

What is the Purpose of Simulation?

SIMULATION TECHNIQUES ALLOW A FICTIONAL YET REALISTIC SITUATION TO be created quickly, easily and economically. Simulation provides a controlled environment that draws its basis from, and interacts with, real life. It educates and trains the participant to think and react quickly and effectively on a number of levels.

Why Use Simulation Technology?

Ultimately, simulators are professional systems that make no concessions to the amateur—simply because there is no room for the amateur in the realm of weapons. If used incorrectly, simulators can be little more than an expensive and amusing video game for adults. However, if used to their fullest potential, simulators represent a unique and invaluable tool in the training and education of security and military personnel.

Operating in real time, with life-sized target projection, in actual shoot/no-shoot scenarios, simulators demand participants to perform at a high level of judgment and accuracy, which is essential for today's military and security personnel. Also, with legal obligations upon members of the security industry steadily increasing, there is, more than ever, a need for these personnel to be trained to a high level of competence in the everyday performance of their duties.

A trainee police officer once remarked that the simulator is the only means of teaching both the law and the use of the gun at the same time. This is perfectly correct, because the simulator can create a situation which will place the trainee in a position where he/she has not merely to react, but also to make a decision. Thus, a scenario may require the weapon to be drawn; it may then require the said weapon to be fired

in defence. Conversely, it may not require any interaction with the weapon at all. These are the kind of choices confronting the trainee in any given scenario.

Yet it should be noted that not all the scenarios employed by simulators are so clear-cut as the above. Real-life situations are rarely black and white in their concerns, and a decision made upon so elementary an assumption may often prove dangerously incorrect. Some scenarios require justification from the trainee, who must not only decide upon the best method of resolving the situation, but must then explain and justify the adopted course of action to the instructor. Should the instructor agree with the trainee's tactics, then a sound judgment reading may then be inserted into the report.

What Constitutes An Adequate Response?

For a response to be truly effective, it depends upon three quite distinct factors:

- the initial decision: to respond, or not respond, with defensive fire;
- the reaction rate (the speed with which the above decision is reached and the response made); and
- the accuracy of the response.

Simulators allow the instructor to measure these qualities. Reaction time, for example, is measured from the time the threat is evident (that is, from the moment the offender either reaches for his weapon, or advances menacingly toward the trainee) and most often demands a response within the space of less than one second.

The brand of training offered by simulators is not limited to mere target practice. The trainee is not expected merely to react, but must also perform a number of other simultaneous functions, which would conceivably be expected in a real life situation. The trainee must give voice commands, may need to take cover so as to ensure personal safety, or may be obliged to call for back-up, should it be considered necessary. The trainee must also constantly assess the situation to ascertain the whereabouts and ensure the continued safety of any innocent bystanders. Furthermore, the trainee must be conscious at all times of the legal obligations should there be cause to draw and fire a weapon.

Will Simulation Technology Replace Live-Fire Technology?

Simulation is much more than a matter of mere marksmanship. Yet the most common misconception regarding simulation technology is that, ultimately, it represents little more than a particularly sophisticated form of target practice.

The truth is quite different. Simulation requires a trainee to be much more than merely a gun: he/she must think, act and speak simultaneously while being placed in a high-pressure situation that is no less convincing than the real thing. This quality—multiplicity of action—represents the single most obvious advantage of simulation technology. Yet the use of simulators should be applied in conjunction with other methods of training. Simulators should be regarded, not as a substitute for real life experience, but simply as a learning tool—realistic, but essentially artificial—to better equip the trainee for a real life situation.

Thus, the fear that simulation technology will eventually replace live-fire training expressed by some weapons trainers is spurious and patently incorrect. It will do so, no more than the use of flight simulators will replace the requirement to fly actual aircraft during pilot training. Simulation should be considered as simply another adjunct to effective learning.

Features of the Firearms Training Systems Inc. (FATS)

In 1991, simulators offer a wide variety of features and services designed to thoroughly teach trainees in a diverse range of situations—many of which are drawn from actual real life precedents. The variety of weapons available for use with the FATS system, for example, is formidable and ranges from ordinary shotguns, revolvers and automatics (which require reloading procedures and include realistic recoil), right through to M16s, M60s and even a Carl Gustav anti-tank rocket launcher. Likewise, the array of judgmental scenarios available for the FATS system is currently in excess of 450 separate situations—including three full disks of branching scenarios, which feature more than one target and which will continue to run until a lethal hit is inflicted by the trainee. With new scenarios constantly being devised, the potential for system expansion is massive, so that a virtual library of scenarios may be built up by instructors.

Most importantly, the FATS system offers a multi-lane training capacity, which allows more than one trainee to engage in training at any given time—an invaluable aid to the large-scale training of teams and departments. This combination of individual and collective training opportunities through a computer-linked multi-lane system is one of the crucial features in the recommendation of simulation technology.

Furthermore, the ease of setting-up firearms simulation systems must be regarded as one of their most attractive qualities. With simulation, successful training exercises are no longer conditional upon such variable environmental factors as poor or unpredictable weather conditions, or inconvenient scheduling. Fully portable and capable of operating indoors, firearms simulation systems are entirely independent of such concerns. They can effectively run 365 days a year, 24–hours a day.

In the case of FATS, instructors require remarkably little training to operate the system effectively, since it is based on a simple and logical push-button method controlled from a low profile remote console. The instructor is equipped with a monitor and communication control, as well as an override option, allowing him/her to take control of the scenario at any time. This can include pausing or cancelling the exercise at any time in order to highlight and correct errors in the trainee's performance. The instructor may also set the level of 'bullet feedback' appropriate to each scenario and weapon, and may record critiques of each separate trainee. In addition, provision is made in the system for statistical comparisons on a larger (for example, departmental) basis.

Feedback to the instructor is both accurate and immediate, delivered on-screen (in the form of displayed computerised 'scoring' procedures) and also via a hard-copy printout on the system's printer unit, which is attached to the instruction console.

The FATS system also offers a range of diagnostic tools to combat and rectify problem areas evidenced by the trainee's performance in each scenario. Furthermore, a valuable extension to the training program is the incorporation of a written report on the scenario to be completed by the trainee immediately after training. The system not only teaches the trainee to respond to a given situation, but also educates in reporting on and accounting for actions to superiors.

The cost savings offered by the FATS system are two-fold: on ammunition and instructor time. By substituting laser fire for live ammunition, live rounds are not expended in a training situation. For poor shooters the 'tracing mode' allows the trainee to actually see whatever shooting technique problem is experienced, allowing errors to be corrected without wastage of rounds (which would have been used needlessly on a live-fire range). Valuable man-hours for instructors are also reduced.

Conclusion

Firearms simulation technology is available in 1991 and will inevitably be an integral part of police future, just as simulation technology is increasingly being employed to train professionals in all walks of life. Yet in many cases, even when adopted, simulation technology is still not being used to its fullest potential. How ironic it is that police might practise as often as once a week for a game of golf or tennis, and yet receive training to cope with situations which could not only threaten our own lives but the lives of many innocent bystanders, as rarely as once a year.

There is no doubting that the legal obligations on those licensed to carry weapons—be they police, militia, or members of the security industry—have increased dramatically over the last five years, to the point where an officer equipped with a weapon is expected not only to perform his duties effectively and safely, but also to be mindful of the potential for vicarious liability actions which may result from their incorrect judgment. This is clearly a question not only of speed or of accuracy, but of sound judgment and reasoning. It is for this reason that firearms training simulators are essential—they do not merely train 'shooters'; rather, they create fully-fledged 'responders'.

COMMAND AND CONTROL: THE COMPUTER AIDED DISPATCH SYSTEM

Senior Sergeant Neil Preston
and
Ralph Saunders
Queensland Police Service

Queensland Police Service Command and Control System

THIS PAPER DETAILS LOCAL AUSTRALIAN DEVELOPMENT AND IMPLEMENTATION of a $2.5 million police Command and Control System and the practical application of the Computer Assisted Dispatch System as developed by the Queensland Police Service. The system uses Hewlett Packard© 9000 Series minicomputers and Model 300/400t workstation screens.

Command and Control is the system designed for normal day-to-day operations of the Queensland Police Communications Centre. It primarily accommodates police assistance calls from the public, but also caters for minor and major incidents, such as gas leaks and airport terrorist action. The system is used in conjunction with the telephone network, the police radio network and other connected computerised services. Important features include the ability to provide management information, utility in crime targeting purposes, and enhanced officer safety features.

The system, in its simplest form, allows operators to record new jobs, verify address locality from a UBD street registry, review address history for officer safety, check for resource availability, and then assign a police patrol to the task or place the task on a job queue for subsequent action. Job tracking, patrol status, radio areas, rosters, messages, management information and reporting are some of the other features of the Command and Control system.

The system provides direct access to the Queensland Police Service's eighteen major systems, including stolen vehicles and other government and interstate law enforcement agency systems; for example, interstate vehicle registrations for New South Wales and Victoria.

Operators, when logging on to the system, have the flexibility to specify screen colour selection, display font, and the format and size of screen windows. Upon shift-

changes, all outstanding work can be handed over to the new operator, and messages may be set for the new operator to read at sign-on stage.

Incorporating Computer Aided Dispatch

This segment will address the development of Command and Control incorporating Computer Aided Dispatch (CAD) from the aspect of a user representative. It will also comment on the old manual system—the system CAD replaced—and outline some of the reasons for adopting CAD.

Work in the communications room in the previous Queensland Police Service headquarter involved the use of a manual card-recording system. This system required individuals to write and time-stamp entries on a cardboard jobcard. This card was then passed to other operators by means of an endless conveyor belt. The manual system centred around three specific functions: being a call-taker or telephone interceptor, a supervisor and communications coordinator, and a radio operator. The telephone interceptor had no technical aids at his disposal, while the communications coordinator and the radio operator had access to a simple patrol-status computer which gave information centred around patrol status movements as updated by the radio operator.

Why the new system?

The inefficiencies of the old system are obvious. Management information was non-existent, the old vehicle-status computer equipment was obsolete, and the computer system could not be easily changed. Police were soon to move to a new headquarters and this seemed to be the most opportune time to embark upon a course of a full Command and Control system incorporating CAD.

In 1988—at the time the analysis of the old manual operating system and subsequent setting of specifications for the new system was being undertaken—Senior Sergeant Neil Preston joined the CAD team in the capacity of user representative. At the completion of the analysis and specification phase, Senior Sergeant Preston then became directly involved in the evaluation of some twelve tendered CAD programs offered to the Queensland Police Service. (At this juncture, there was an inability to modify existing procedures to accommodate a proposed CAD system as the Queensland Police Service was being examined by the Fitzgerald Commission of Inquiry.)

These evaluations concluded that none of the CAD systems on tender met the Queensland Police Service requirements exactly. This, of course, was to be expected. What had not been expected was the degree of fit of those offered and the degree of difficulty and expense of modifications to meet those requirements. The fit ranged from an estimated 30 per cent to 85 per cent but the bulk of systems rested in the 50 per cent to 60 per cent range. The system which came close to the needs of the Queensland Police Force was from an American supplier. However, this system was not accepted because:

- the supplier had no Australian backup or representation;
- licence fees applied for each location the program was to be sited;
- high cost of initial change and any further changes could only be carried out by the supplier;
- copyright would always remain with the supplier regardless of the extent of the changes; and
- other technical reasons.

It was interesting to note that no two CAD systems offered for evaluation could be considered the same.

For several reasons, it was decided that an existing CAD system would not be utilised, but that the Queensland Police Service would undertake to write a CAD program specific to its requirements.

The plan

In May 1989, the Queensland Police Service made the decision to accept the solution proposed by Telecom Australia. This solution involved:

- the Queensland Police Service;
- *Telecom* (to be engaged as the Prime Contractors and Project Managers);
- *Hewlett Packard* (to provide the operating systems, LAN software and resilient hardware);
- *BHA Computer* (system builders and system integrators);
- *Sybase* (to provide relational database software); and

  KPMG (to provide system and organisational reviews).

Subsequent to the initial specifications, prototyping commenced in September 1988. This opportunity was taken to incorporate into the prototype computer solutions to some of the inherent problems associated with the old manual system, the most prominent of those problems being:

Allocation of resources

- similar jobs: there can be nothing worse than allocating two or more patrols to a single job which requires the attendance of no more than one patrol. This frequently occurred when two or more jobcards were written on the same incident and were not matched as the same job.

- suggested patrols report: the allocation of resources based on geographic location had always presented extreme difficulty in the old manual system.

Addresses

- address history: the ability to gain information regarding prior police attendances at specific addresses.

- address intelligence: the ability to flag a specific address with intelligence data.

- address validation: the ability to validate addresses at the point of entry.

- common place names: the ability to store address information relating to specific or common place names.

The prototype was duly completed incorporating not only these, but many innovative ideas, thereby establishing a base platform from which the system was to be extended by BHA Computer.

The system commenced operation on the 10 September 1990 and future plans include two major sub-systems: tows, and messages through the ICL mainframe computer network.

Reviewal of the new system

The System is continuing to be reviewed. Two of the higher priority issues include: resolving cases of lumpy performance; and reviewing the role of the communications coordinator. Documented change requests are noted, awaiting attention, and further development of the system will cater for:

- mobile terminal facilities for beat and vehicle patrols to reduce radio airtime estimated to be in the vicinity of 30 per cent, provide direct access to existing databases and enhance police officer safety;

- provision of mapping facilities for major and minor incidents;

- call line identification, initially for emergency calls only;

- an executive information system, in addition to the current reports which are now available as a feature of the current system; and

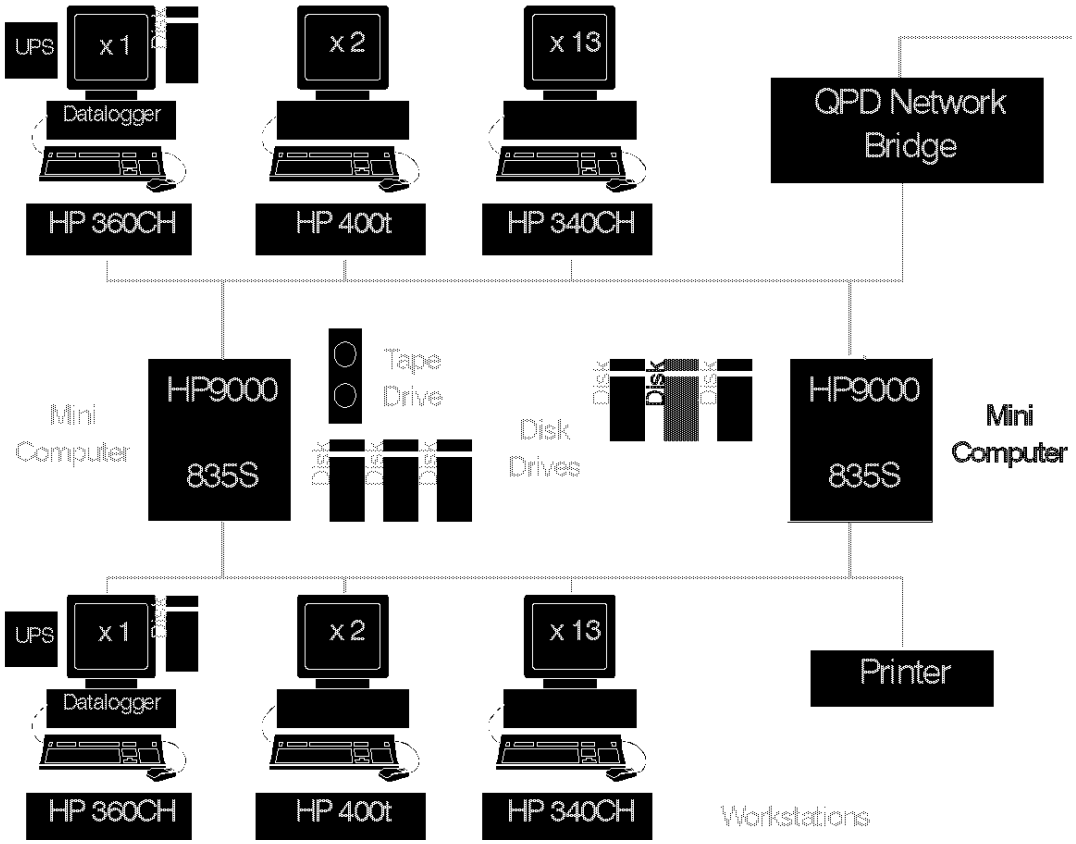
- expansion of the system to other police regions throughout Queensland. (The South East region with a target site of the Gold Coast is an appropriate site for initial expansion of the system.)

Computer System Architecture

The computer hardware of the Command and Control CAD system comprises dual Hewlett Packard© minicomputers along with two Hewlett Packard© 360 workstations as 'boot nodes' for starting the application which also act as logging devices. There are six gigabytes of disk storage and tape and printer devices. Figure 1 shows an outline of the full production configuration.

Figure 1

Queensland Police Service Command and Control System Configuration Diagram



To provide resilience, two separate-but-linked local area networks (LANs) have been installed and fifteen diskless workstations are connected to each LAN for the system operators. Ten workstations are installed in the Major Incident Room and twenty workstations in the Police Communications Centre. A separate linked Development System is now available.

The UNIX operating system HP-UX7, and Arpa/Berkley and NFS network services are used over the ethernet LAN. The application is written in SQL and the 'C' programming language, with stored procedures and X11 Windows is used for the workstation user interface. Jobs and other details are stored in the relational database from Sybase.

To present a consistent interface to our police users, a VT220 emulator from Optimation Inc. has been incorporated into the application. The operator workstation

screens are nineteen inch large-size, bit-mapped, multi-colour screens. The hardware reliability has been excellent.

Since commencing live operation on the 10 September 1990, there have been twenty-seven scheduled breaks of an average of one-and-a-half hours duration each. These scheduled breaks include new releases of application software and systems maintenance.

Unscheduled downtime covers operator errors, logs filling up, and problems with the application code and database. The longest outage was for fourteen hours on 27 October 1990. Since December 1990 through to September 1991, the CAD system has averaged less than two hours unscheduled downtime per month (that is, four minutes in every 24–hour period).

THE USE OF CIE COLOUR COORDINATES IN FORENSIC SCIENCE

Elizabeth Kostantakis
and
Professor Michael Pailthorpe
Department of Textile Technology
School of Fibre Science and Technology
University of New South Wales

THE TEXTILE DYEING AND PRINTING INDUSTRY, ALONG WITH OTHER COLOUR using industries (paint, food, plastics, ceramics and cosmetics) have adopted CIE-based colour systems for colour specification, colour formulation (recipe prediction), colour difference specification and quality assurance procedures. In the textile industry, objective colour measurement has been in use since the 1950s. Recent developments in computer technology, combined with the low cost of powerful personal computers, has meant that in 1991 virtually all dyehouses have a dye recipe prediction system. The Society of Dyers and Colourists (UK) have recommended the CIEXYZ colour space for colour specification and the CIELAB colour space for colour difference specification. The extensive sample colour databases held by dyers might, therefore, be useful in the forensic examination of coloured fibres.

As a direct result of the widespread adoption of instrumental colour match prediction, together with economic and environmental pressures, dyestuff manufacturers have rationalised their dyestuff ranges. They will now recommend trichromatic combinations of, say, a red, yellow and blue for colour match prediction databases. This means that it is now more likely for a combination of the same three dyes to be used for the formulation of many colours on the one substrate. The consequences of this trend to forensic science were recently discussed by Pailthorpe (1990).

Colour match prediction systems employed in the textile industry comprise an abridged reflectance spectrophotometer coupled to a powerful personal computer operating with appropriate software. The spectrophotometer will normally have a

sample aperture of circa 20–30 mm. The measurement geometry is usually diffuse CIE D65 illumination, specular excluded with 8–15° observation.

In the forensic examination of fibres, a microspectrophotometer is employed to measure the transmission of light through the individual fibres. Microspectrophotometry is usually employed as part of the fibre selection/rejection process which is followed by some form of extraction and chromatography of the extracted dyes. In the past, fibre colour comparisons using a microspectrophotometer have been made on the basis of comparing the shape of the normalised absorbance curves of the control and crime scene fibres. This can be achieved by an overlay technique or some form of least squares type analysis.

Some attempts have been made to use CIE coordinates in forensic science. Many workers (*see* Grieve, Dunlop & Haddock 1988; Rounds 1969; Laing, Hartshorne & Harwood 1986; Hartshorne & Laing 1988; Paterson & Cook 1980) have used the so called Complementary Chromaticity Coordinates (CCC) to describe colour. This system is based on a paper by Rounds (1969), who describes a method by which the CIE distribution coefficients and CIE illuminant spectral power distributions are applied to absorbance values rather than the transmission values. Whilst this may be a mathematically convenient approach, the CCC's have no meaning whatsoever in terms of the stimulus to the human eye.

With this background in mind, the aim of this work was to examine two aspects of the application of CIE chromaticity coordinates in forensic science:

- is there any correlation between the CIE coordinates measured in reflectance on abridged spectrophotometers (as used in the textile industry) and those determined in transmission on microspectro-photometers? and

- are the mathematically convenient CCC's any better than the true CIE chromaticity coordinates for use in forensic science?

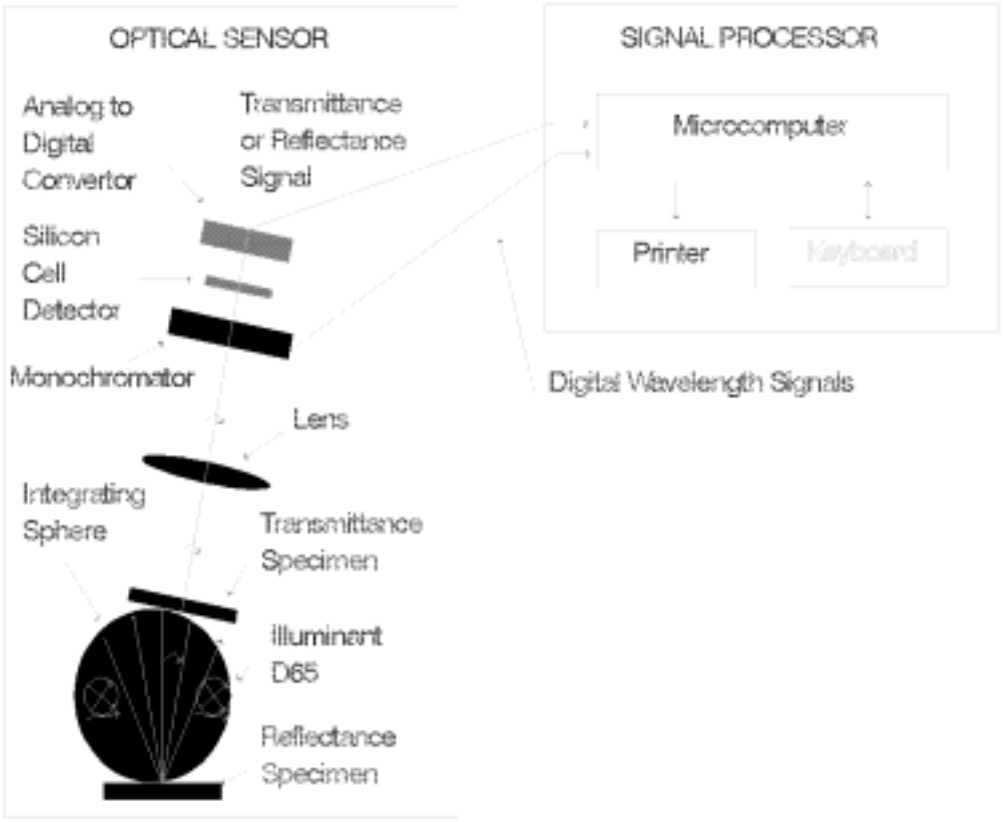
Experiment

Instruments

Macroscopic colour measurements were made using a Pacific Scientific Spectrogard Colour Computer System. The optical layout is given in Figure 1. The sample is illuminated with a diffuse CIE D65 source through a 20 mm diameter aperture. Observation is at 8° with the specular component excluded. The illumination/viewing geometry is therefore diffuse/8°. The Spectrogard software calculates the CIE chromaticity coordinates for the 10° observer over the spectral range 380–720 nm. The reported results are the means of four measurements made on randomly selected areas of the dyed fabrics.

Figure 1

Optical Layout of the Spectrogard Colour Computer



Microscopic measurements were made using an Olympus DMSP–II UV–Visible microspectrophotometer. The instrument was connected to a personal computer running data capturing software written by Mr J. Wickham of JRAK Biosignals. The optical layout is given in Figure 2. The fibre sample is viewed in transmission with a fourteen micron circular monochromated beam. The illumination/viewing geometry is therefore 0°/180°. Measurements were made over the visible spectrum from 400–700 nm. The spectral data was then converted to CIE and CCC coordinates (10° observer) by a purpose-written computer program (Kostantakis 1991). The reported results are the means of at least six measurements made on randomly selected fibres sub-sampled from the dyed fabrics.

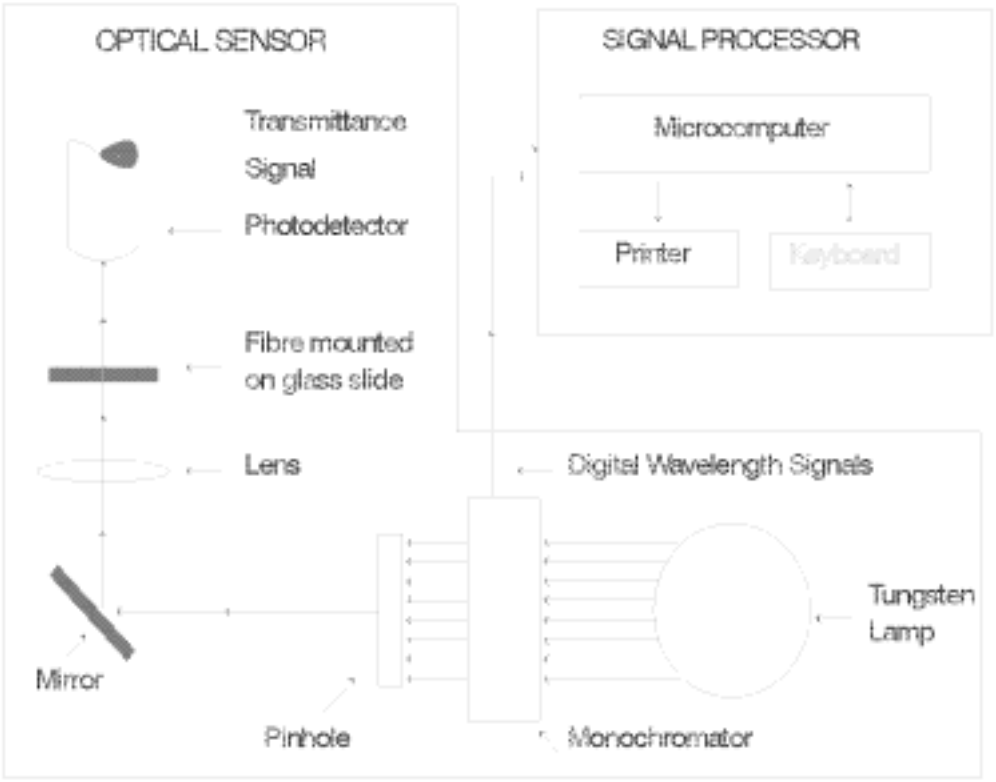
Samples

Clear and coloured cellophane films were purchased from a local newsagent. The wool fabric used in this work was a scoured and decatised plain weave worsted fabric of 180 g/m^2. The wool fabric was dyed with combinations of the trichromatic dyes Drimalan Red FBR, Drimalan Golden Yellow F3RL and Drimalan Blue FGRL using the Sandoz *Temperature Stop Process* (Sandoz Drimalan F Pattern Card 1509/70). In addition, four dyed wool fabrics were purchased from retail outlets in Sydney. In this way a range of ten shades

from red to purple was obtained. The dyed fabric samples were employed for colour measurement on the Spectrogard while fibres were subsampled from the fabrics and mounted on microscope slides for measurement in the microspectrophotometer.

Figure 2

Optical Layout of the Olympus Microspectrophotometer



Results

Cellophane trials

Coloured cellophane was employed to examine both the reproducibility of the microspectrophotometer and to test for the existence of a correlation between measurements made in reflectance and transmission on the Spectrogard.

The microspectrophotometer was found to be very stable and to give reproducible results on a day-to-day and week-to-week basis. The 95 per cent confidence limits in CIE x and y were 0.0005 and 0.0009 respectively for blue cellophane, and this was typical of the other coloured cellophanes employed. The reproducibility in measured CIE (x,y) chromaticities from week to week was also found to be very good. Typical week to week results for the CIE (x,y) coordinates are given in Figures 3 and 4.

Figure 3

CIE x Coordinates Measured One Week Apart on Cellophane Using the Olympus

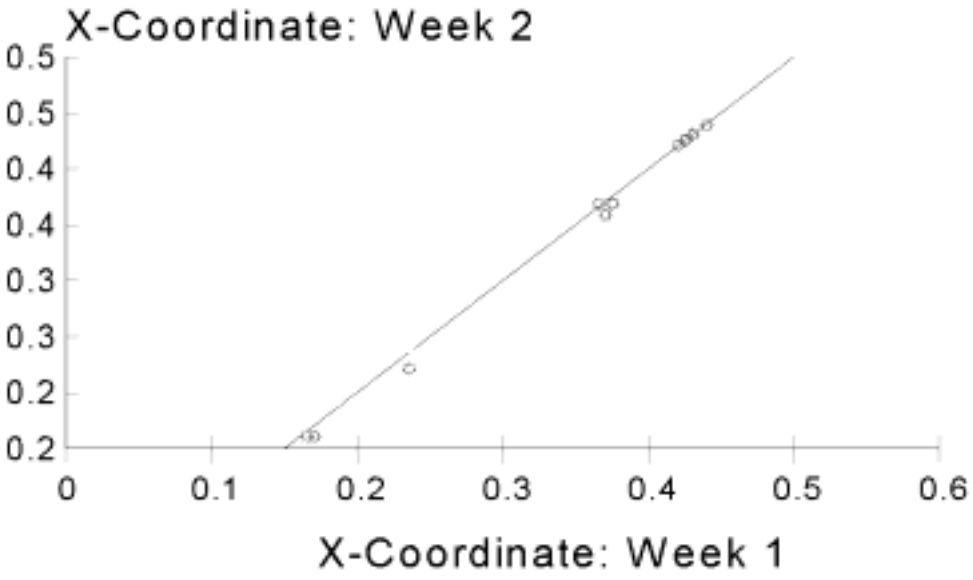
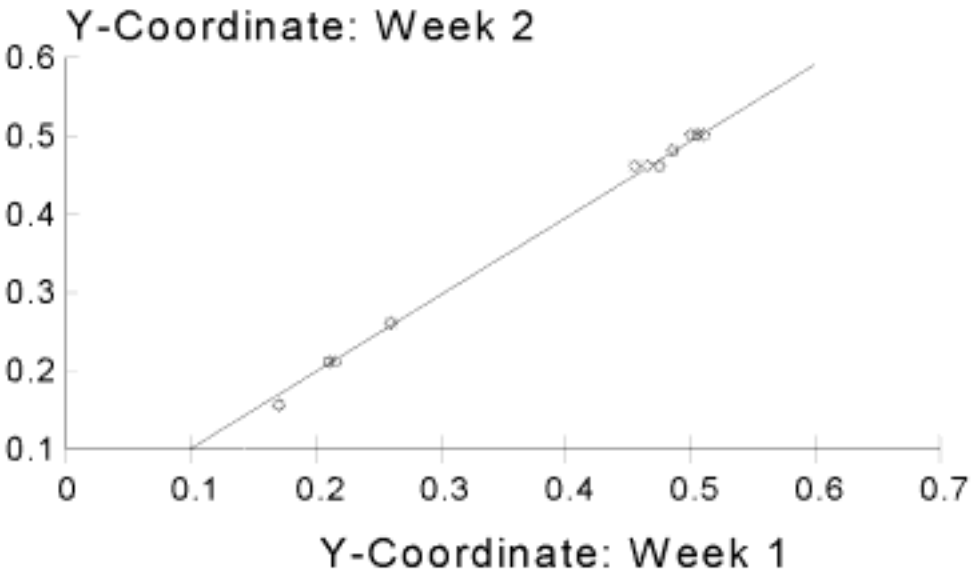


Figure 4

CIE y Coordinates Measured One Week Apart on Cellophane Using the Olympus



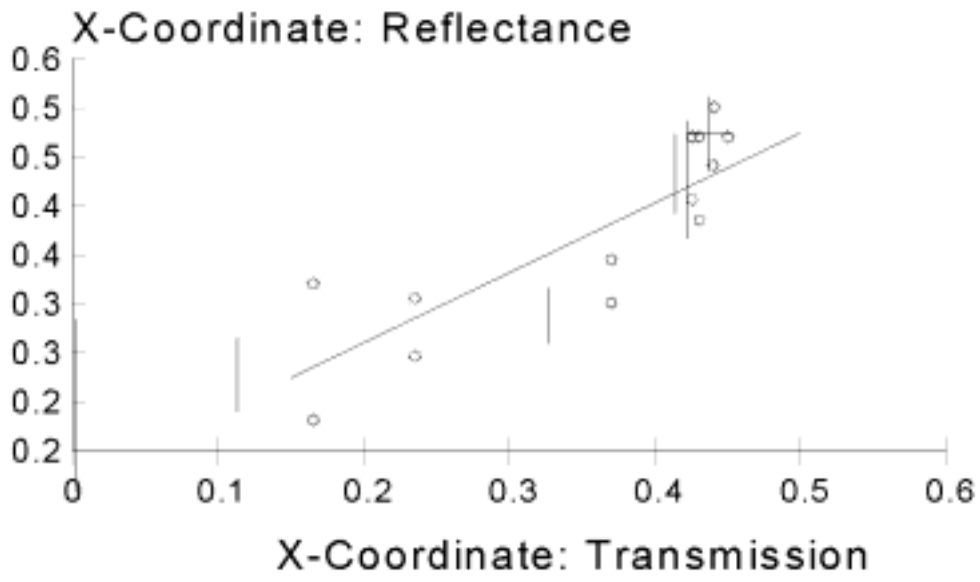
Note: Error regions included in Figures 3 and 4. R–square = 0.996.

It can be seen that the results are highly reproducible with a correlation coefficient of 0.996. This result is very good when one considers that coloured cellophane is not 100 per cent homogeneous when viewed at the microscopic level (fourteen micron beam size).

The cellophane films were then measured both in transmission and in reflectance on the Spectrogard. A typical result is given in Figure 5 for the CIE x coordinate. A similar plot was obtained for the CIE y coordinate. Statistical analysis of these data showed that very few of the chromaticity coordinates 'matched' at the 95 per cent confidence level. Thus there is very poor agreement between CIE (x,y) chromaticities measured in transmission and reflectance on the same instrument.

Figure 5

CIE x Coordinates Measured in Transmission and Reflectance on the Spectrogard



Note: Error regions included. R–square = 0.81.

Dyed Wool Fabrics

CIE (x,y) coordinates

Typical data for the CIE x coordinate measured in both reflectance and transmission are plotted in Figure 6. A similar plot was obtained for the CIE y coordinate data. It can be readily seen from the data in Figure 6 that the 95 per cent confidence limits in

the mean values of the CIE x coordinate measured in transmission are very large. This large confidence limit arises as a direct result of:

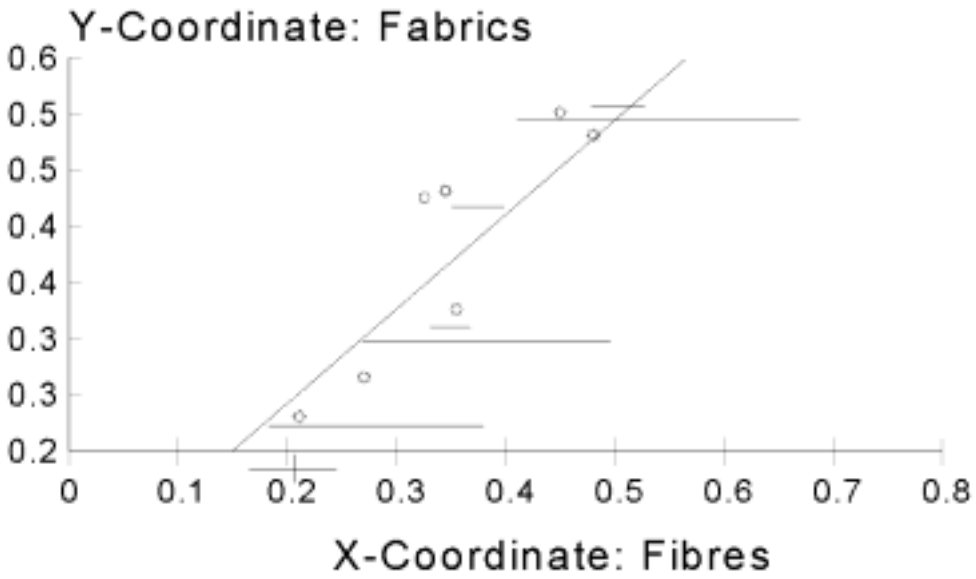
- microscopic variations in the distribution of dyestuff within and between fibres;
- variations in path length (fibre diameter) within and between fibres; and
- changes in chromaticities with dyestuff concentration (Giles 1971).

The 95 per cent confidence limits in the mean values of the CIE x coordinate measured in reflectance are much smaller, being a direct result of the large sample aperture used for measurement.

Statistical analysis of the data has shown that, at the 95 per cent confidence level, the CIE (x,y) coordinates measured in reflectance do not 'match' the CIE (x,y) coordinates measured in transmission. The correlations between the data are also poor (*see* Figure 6).

Figure 6

CIE x Coordinates for Fabrics in Reflectance and Fibres in Transmission



Note: Error regions included. R–square = 0.74.

Complimentary Chromaticity Coordinates (CCC)

The CCC (x,y) coordinates were then calculated from the transmission data obtained on the microspectrophotometer. Statistical analysis of the CCC data was carried out

and the 95 per cent confidence limits in the mean CCC (x,y) coordinates compared with the 95 per cent confidence limits in the mean for the CIE (x,y) coordinates. Some typical results are given in Table 1.

Although the (x,y) chromaticities cannot be directly compared, the confidence limits in mean values of the (x,y) chromaticities can be compared. It can be seen that the 95 per cent confidence limits in the mean CCC (x,y) coordinates are generally on a par with or greater than the 95 per cent confidence limits in the mean values of the CIE (x,y) coordinates. These results are typical of data spanning a wide range of hues. Hence it would appear that CCC coordinates have little to offer over standard CIE (x,y) coordinates for the representation of the colour of microscopic samples.

Table 1

A Comparison of CIE and CCC Coordinate Systems

Sample	Parameter	Complementary Coordinates	CIE Coordinates
Undyed Wool	x	0.2371	0.3278
	Δx	0.0852	0.0150
	(%)	(35.9%)	(4.6%)
	y	0.2255	0.3498
	Δy	0.0810	0.0154
	(%)	(35.9%)	(4.4%)
Red Wool	x	0.2757	0.3465
	Δx	0.0260	0.0161
	(%)	(9.4%)	(4.6%)
	y	0.4210	0.2775
	Δy	0.0497	0.0196
	(%)	(11.8%)	(7.1%)
Purple Wool	x	0.3513	0.2684
	Δx	0.1071	0.0794
	(%)	(30.5%)	(29.6%)
	y	0.4145	0.2382
	Δy	0.1342	0.0792
	(%)	(32.4%)	(33.2%)
Orange Wool	x	0.2111	0.4799
	Δx	0.0586	0.1041
	(%)	(27.8%)	(21.7%)
	y	0.2473	0.3806
	Δy	0.0825	0.1134
	(%)	(33.4%)	(29.8%)

Table 1 cont'd

Sample	Parameter	Complementary Coordinates	CIE Coordinates
Blue Wool	x	0.4303	0.2072
	Δx	0.0581	0.0295
	(%)	(13.5%)	(14.2%)
	y	0.3964	0.2465
	Δy	0.0518	0.0349
	(%)	(13.1%)	(14.2%)

Note: Δx represents the 95% confidence limit in the mean value of x. Δy represents the 95% confidence limit in the mean value of y. The (%) values represent Δx/x and Δy/y expressed as percentages.

Conclusion

CIE (x,y) chromaticity coordinates measured in transmission on fibres in a microspectrophotometer do not agree with the CIE (x,y) chromaticity coordinates measured on fabrics in an abridged spectrophotometer. Thus it would appear that the colour databases held by dyers will be of little use in forensic science.

The CCC (x,y) chromaticity coordinates calculated for fibres in this study generally have errors either equal to or greater than those for the standard CIE (x,y) chromaticity coordinates for the same fibres.

The wool fibre database has recently been extended to include an additional twelve hues and it was found that the new data fully supports the conclusions made herein.

Therefore it would appear that, for the time being, the application of CIE (x,y) chromaticity coordinates in forensic science is limited to colour comparisons on fibres of the same dyeing depth and measured under identical geometrical conditions.

References

Giles, C.H. 1971, *A Laboratory Course in Dyeing*, The Society of Dyers and Colourists, Bradford, UK.

Grieve, M.C., Dunlop J. & Haddock, P. 1988, 'An Assessment of the Value of Blue, Red and Black Cotton Fibres as Target Fibres in Forensic Examinations', *Journal of Forensic Sciences*, JFSCA, vol. 33, no. 6, pp. 1332–44.

Hartshorne, A.W. & Laing, D.K. 1988, 'Colour Matching within a Fibre Data Collection', *Journal of Forensic Sciences*, JFSCA, vol. 33, no. 6, pp. 1345–54.

Kostantakis, E. 1991, An Evaluation of the Application of CIE Colour Specifications in Forensic Science, Honours Thesis, University of New South Wales.

Laing, D.K., Hartshorne, A.W. & Harwood, R.J. 1986, 'Colour Measurements on Single Textile Fibres', *Forensic Science International*, vol. 30, no. 1, pp. 66–77.

Pailthorpe, M.T. 1990, 'Recent Developments in the Colouration of Fibres Encountered in Forensic Science Examinations', presented at the Twelfth International Conference on Forensic Sciences, Adelaide, Australia.

Paterson, M.D. & Cook, R. 1980, 'The Production of Colour Coordinates from Microgram Quantities of Textile Fibres', *Forensic Science International*, vol. 15, pp. 249–58.

Rounds, R.L. 1969, 'A Colour System for Absorption Spectroscopy', *Textile Chemist and Colourist*, vol. 1, pp. 297–300.

AUTOMATED FINGERPRINT SYSTEM

Don Toews
National Projects Manager
NEC Information Systems Australia
New South Wales

EVER SINCE THE INTRODUCTION OF COMPUTER SYSTEMS, THE CAPACITY TO revolutionise the searching of fingerprints has been recognised as one of the key areas that would provide tremendous benefits to law enforcement agencies around the world.

Australia first introduced the process of fingerprinting into the gaols some ninety years ago. A central Fingerprint Bureau was established in 1941 in Sydney in an effort to consolidate the processing of interstate criminal identifications. Since that time, the need for fingerprint identification in solving crime has grown beyond the practical limitations imposed by human capability. Over time the process became overloaded with the demands of crime scene activities, and thus the computerisation process became the only viable alternative.

In 1986, the Australian Police Forces implemented one of the largest Fingerprint Identification Systems in the world. Since that time, the system has expanded across the nation to incorporate over 1.7 million fingerprints. This remarkable achievement could only have been made possible as a result of a national cooperative effort of the various police forces. The technology employed is unique in all aspects of computing and, therefore, does not lend itself to commercial computing systems. The techniques were developed in conjunction with fingerprint experts and are based on world standards set for fingerprint identification.

The success of the system can be attributed to the high standards established for quality fingerprint input at time of conversion, and the motivation generated by the system as a result of successful fingerprint searching. Previously, 10 per cent of crime scene latent fingerprints were searched against 6 per cent of the main file whereas, in 1991, the total database is accessible by all fingerprint workstations around Australia, at any time of day or night.

The future of fingerprinting in law enforcement will focus on the two main areas of improved quality, namely: at the time of arrest and on crime scene attendance, through the implementation of direct electronic fingerprinting. The expansion of the fingerprinting process into other commercial applications of identification and security will only enhance the level of importance attributed to the technology in Automated Fingerprint Systems.

INFORMATION TECHNOLOGY: WHERE IS IT IN THE COORDINATION OF EMERGENCY SERVICES?

Peter S. Anderson
Research Fellow
Centre for International Research on Communication and Information Technologies (CIRCIT)
Melbourne
Victoria

THE APPLICATION OF NEW COMMUNICATION AND INFORMATION TECHNOlogies opens up opportunities for significant improvements in integrating, coordinating and communicating information among emergency services. The need for such communication is especially critical where emergency services are called upon to manage the effects of major emergencies and disasters. Although often local in origin, the impacts of such events usually spread across social as well as physical boundaries, requiring multi-agency response and resource allocation. Furthermore, the adequacy of response is greatly influenced by the degree to which organisations and individual respondents can collectively develop and implement solutions to commonly recognised problems and associated responsibilities (Anderson 1990a).

However, neither recognising common problems, nor developing and implementing common solutions are easy tasks. Firstly, hazards and their effects are continuously changing in kind and in their effects on human populations. The increased urban use of hazardous chemicals, for example, combined with poorly designed storage facilities and transportation routes can easily place large concentrations of people at risk. So can the effects of natural disasters—especially where large numbers of people are concentrated in inadequately planned and poorly protected environments.

Secondly, a close relationship can often be found to exist between those hazards identified at local, national and international levels, whether they be climatic, geophysical, biological, technological or a function of the interaction between them. As economies and cultures become more interconnected through globalised transportation and communication systems, growing interdependency also means that disasters occurring in one region of the world may have significant effects on others.

Thirdly, given these interdependencies and a growing specialisation in hazard management, no single organisation can be expected to be able to identify or address all of the consequences of hazard occurrences. Rather, the breadth of information required to formulate options and make critical decisions about hazards is considerable, requiring the input and integrated efforts of a number of jurisdictions and disciplines including law, medicine, government and non-government services, technical and social sciences (Anderson 1990a).

When disasters do happen, there is a need to exchange large amounts of information in order to determine: what has happened, what is happening and what is likely to happen; threats to life, property and the environment; numbers and locations of personnel and physical resources required; numbers of people affected and their immediate needs, and so on. In such a rapidly changing environment, information gathering, interpretation and communication must be done quickly to ensure that decision-making remains timely and responsive. This requires the use of efficient and complex exchange mechanisms which often must bridge local, national and international communities of interest and cultures.

Moreover, research has shown that the benefits of cooperation among emergency services under such conditions can be significant, and can lead to greater operational efficiency through avoidance of material waste and/or loss of time and effort, greater effectiveness through a more balanced and timely distribution of common resources, and improved intra and interorganisational relations.

The Role of Communication and Information Technology

The application of new communication and information technologies (CITs) may provide new opportunities for integrating and improving the exchange of information across organisations, activities and geopolitical boundaries, not only for enhancing disaster preparedness, response and recovery operations, but also for facilitating better preventive and mitigative efforts. In fact, the application of CIT in disaster management is already apparent in many forms including the use of remote-sensing satellites, electronic databases, electronic messaging and geographic information systems.

Emergency services make extensive use of many of these types of services over local and wide area networks, in similar ways that they have become accustomed to relying upon telephone voice, teletype, facsimile, two-way radio and electronic broadcasting services. Additionally, space technology provides valuable back-up and alternative fixed and mobile communication across vast regions of the planet.

Despite these improvements, however, the application of CIT in disaster management still tends to evolve nationally and internationally in a fundamentally uncoordinated fashion. Further, despite the enormous outpouring of research from the global scientific community, little of this effort appears to be making its way into policy or operations, with the result that social benefits, in the form of improved disaster mitigation, are yet to be realised (Cochrane 1991).

Efforts to coordinate and direct response and recovery operations also remain problematic. More often than not, the communication infrastructure required to facilitate such operations is one of the first victims of a disaster. The telephone network, in particular, is vulnerable not only to physical damage, but also to congestion which can slow down or prevent emergency organisations from contacting and communicating with each other. The same problem exists with cellular radio telephone services. Although a portable medium, cellular radio is primarily an extension of the public switched telephone network and, as such, is susceptible to the same kinds of problems. Base stations and/or radio repeaters remotely connected to dispatchers via dedicated land-lines can be equally vulnerable to disruption by physical damage (Anderson 1990b).

Despite these potential set-backs, emergency services generally appear to be becoming more dependent upon land-line based networks rather than seeking alternatives or ensuring that such facilities are strengthened through better protection, redundancy and diverse routing. While integrated radio-based technology would appear to be among one of the most obvious alternatives, most organisations are constrained by limited organisational and financial resources and radio spectrum. Another problem is the tendency to design radio networks primarily to facilitate intraorganisational communication, with insufficient attention paid to interorganisational requirements. This often results in one emergency service being unable to communicate—or communicate effectively—with another because of incompatible radio systems or lack of familiarity with each others' operating procedures and facilities.

Furthermore, the scope of radio usage may be limited because of physical blockage of signals, noise, intermodulation, poor signal propagation or inadequate power supplies. Shortcomings are also evident where duplex base stations or repeaters become inoperable, and remaining radios are incapable of simplex or single frequency operation.

Finally, there is the problem of organisations called upon to support emergency services not possessing any reliable communications facilities at all, or being unable to communicate directly with emergency operations centres. Some organisations, such as the Red Cross, in fact, may be volunteer based and have communication and information requirements that are greater than those of many of the regular full-time emergency services.

Fortunately, in many countries there are amateur radio organisations like Australia's Wireless Institute Civil Emergency Network (WICEN) that, when properly trained and supported, can help to restore lost links, extend networks across organisations, and expand network capacity when required. They are also capable of operating across many different frequency bands both nationally and internationally and are among the most innovative users of analogue and digital radio telephony. To ensure that their role in disaster management can be effective, however, means that they must be accepted and supported as active participants in disaster planning as well as in disaster response and recovery operations.

In light of these issues, there is an obvious need for improving communication and information infrastructures both within individual and across emergency services. While no doubt there are a variety of technical solutions to many of the problems outlined, the impact of these solutions may be negligible unless a number of significant economic, political, social and professional issues are also addressed to ensure that solutions proposed match with perceived need, expectations and organisational capabilities. These requirements can best be done before disasters

occur, through defining intra and interorganisational needs and problems, identifying appropriate sources of information, and developing ongoing methods of information exchange which can assist in satisfying these needs.

Toward an Integrated Australian Disaster Management Information Network

Project impetus

In an effort to strengthen disaster management networks in Australia and abroad, the Centre for International Research on Communication and Information Technologies (CIRCIT) and the Australian Counter Disaster College (ACDC) established a working relationship in late 1989. In July 1990, CIRCIT and ACDC co-hosted a week-long workshop at the College in Mount Macedon, Victoria, to assess information exchange needs within the Australian counter disaster community[1]. The workshop drew upon the talents of some thirty-five experts from across Australia and abroad who collectively represented all key elements of the disaster management process—prevention, mitigation, preparedness and recovery.

The aims of the workshop were to identify and analyse the nature and range of information exchange needs within the Australian counter disaster community, the effectiveness of current means used to exchange such information, and to recommend changes (including the possible use of new technologies) to increase the effectiveness of current information exchange practices; and to propose implementation strategies. After studying these issues, workshop participants recommended a number of solutions and implementation strategies, including:

1 The term 'counter disaster community' is used to encompass anyone or any organisation involved in activities related to the prevention or mitigation of, preparation for, response to, or recovery from major hazard occurrences. Such a community includes practitioners, researchers, facilitators, government and non-government organisations, as well as affected or interested members of the public.

- expansion of counter disaster related research activities and dissemination of results;
- establishment, promotion and maintenance of an Australian disaster database;
- development of improved communication techniques between all elements of the counter disaster community, especially with the general public;
- establishment of arrangements to ensure effective feedback between stakeholders; and
- establishment of active information collection arrangements to:
  - identify user requirements for new technology;
  - evaluate new technology; and
  - highlight, evaluate and disseminate information on new techno-logies (Anderson 1991).

For these particular tasks it was recommended that ACDC and CIRCIT, in collaboration with other organisations, play a lead role in facilitating and coordinating projects.

Australian Disaster Management Information Network working group

In September 1990, a working group was established with a view to exploring avenues for implementing the above recommendations and, in particular, to initiate a pilot project in order to examine what specific role an electronic information exchange network might play in such implementation. Taking into account the geographical proximity of the project's initiators, as well as the necessity to gain knowledge about local and regional dimensions of information exchange before extending linkages nationally and internationally, it was decided that the scope of the initial scope of the project would be limited primarily to Victoria. In addition to ACDC and CIRCIT involvement, participation in these activities currently includes:

- Community Services Victoria (State Recovery Unit);
- Victoria Country Fire Authority;
- Melbourne Metropolitan Fire Brigade;
- Victoria Police (State Disaster Planning Office);
- Victoria State Emergency Service;
- Wireless Institute Civil Emergency Network;

- Eastcom Pty Ltd; and
- the City of Williamstown.

It is expected that participation will be broadened considerably, once the pilot project is fully-activated.

Since the inaugural meeting, a number of issues have been discussed about the content and management of a computer network, as well as technical considerations. During initial discussions, it soon became clear that CIT usage and experience varies considerably within the counter disaster community. As such, there was an early realisation that the design of the pilot project must take account of the fact that some prospective participants may have little or no computer experience. Further, concerns have been raised that the system/user interface should be very 'user friendly', yet be flexible enough to allow more experienced users additional features, as well as being adaptable to future innovation.

Another concern is that the content and its organisation and presentation must be relevant to users and should, as much as possible, be tailored to reflect basic counter disaster principles and practices. Yet another concern is that, in order to encourage a wide range of participation, the technical and cost requirements for accessing and using the network must be minimal, since few participating organisations or individuals are likely to have additional resources for experimentation.

Taking into account these events and concerns, a pilot network project commenced in June 1991. The design, operation, contents and maintenance of the network are being determined, in part, through an analysis of existing systems and through consultation with the Australian counter disaster community. In light of this ongoing process, many of the project parameters are designed to remain flexible, so as to allow adjustments to be made according to experience gained throughout the project. As such, the following brief overview reflects current planning, and may vary with subsequent implementation.

Australian Disaster Management Information Network (ADMIN)
Project Description

The project entails designing and implementing an information network that relies upon personal computer-based bulletin board technology to form the core of the network, while also being capable of interconnecting to other computer networks where relevant. Emphasis has been placed on utilising and/or supplementing existing organisational resources, rather than promoting the development of entirely new concepts and practices. When fully established, the network will facilitate exchange of electronic mail between participants, automatic mail-forwarding between sites, and ongoing electronic conferences on subjects common to various groups.

The network's chief purpose is to serve as a central source of timely information about counter disaster organisations and their activities, training courses and instructional materials, disaster and hazard research, conference papers and newsletters, literature lists, public and private sector information services, calendars of events, contacts and on-line databases.

The results of the project are expected to provide greater understanding of the role that readily available communication and information technologies can play in facilitating coordination and integration of disaster management practices, as well as how more efficient employment of CIT can be effected within organisations. For

ACDC, this project will also provide an opportunity to examine and evaluate options for expanding access to its training and information services.

Phase I: development of ADMIX

Phase I of the project entails placing on-line a computer conferencing system entitled the Australian Disaster Management Information Exchange (ADMIX). ADMIX is a microcomputer-based system that utilises existing off-the-shelf computer equipment and state-of-the-art electronic mail and information management software. The software is already widely used throughout the world, and technical support for its use can usually be found in most communities.

The system's content and user features are easy to customise, as are links to other sites. Portions of the system have been set aside for specialised areas of interest, including personal and general messaging, ACDC activities and services, research, electronic conferences on topics related to prevention/mitigation, preparedness, response and recovery topics, as well as international activities.

Access: Access to the service is facilitated over existing telephone networks. The only equipment required to access ADMIX is a personal computer, communications software and a modem. Although ADMIX operates on an IBM-compatible personal computer system, the system can be accessed by virtually any type of system that supports standard ASCII text and other common data transfer protocols. The system is available 24–hours a day, except during early morning hours, or occasionally during the day when the system is exchanging and processing data with other systems or is off-line for maintenance.

Training: Because computer/communication usage and experience varies considerably within the counter disaster community, ADMIX has been designed to cater to those who possess minimal knowledge of computing, yet is flexible enough to allow experienced users additional features. The system is menu driven, allowing the user to easily move around within the system and to activate various features, often by simply typing single letters to execute computer commands. ADMIX also provides special on-line help features for each command and user function, as well as a special conference area to allow users to discuss ADMIX technical matters and to propose system improvements. Copies of a user manual are also available upon request.

Cost: In addition to the cost of a personal computer, communications program, and a modem, the only significant direct costs are STD expenses (for telephone line access). For most organisations, personal computers are already available, requiring only the acquisition of a modem and communication program. Like the bulletin board software used in this project, communication software is available both in commercial and non-commercial forms. For those who wish to become regular content contributors, additional costs may be incurred in converting information into a suitable computer format. Every effort will be made to encourage users to contribute new information, rather than to simply copy data from the system.

Links to Other Sites: During the course of the project, ADMIX will be linked to other associated systems to form a data network based on similar technology. This arrangement will allow users to experiment with automatic mail and other data forwarding to other sites, and conferencing across systems (wide area networking), as well as to examine

requirements for managing and coordinating future network expansion. Currently, ADMIX is linked to systems operated by the Wireless Institute Civil Emergency Network (WICEN), Southern Mail and CIRCIT (all of which are located in the Melbourne area) and the Emergency Preparedness Information Exchange (EPIX) in Vancouver, Canada. Other Victorian counter disaster organisations have proposed establishing their own nodes, as have organisations in other states.

A national electronic addressing scheme has been developed to accommodate these additions. This scheme allows each site or node to have its own unique address, so that network links for automatic mail forwarding and conferencing can be easily facilitated across different segments of the network. It is expected that each site's content and user features will be customised to reflect the interests and needs of the organisation managing it, while, at the same time, through message exchange and conferencing links with other nodes, will also reflect many common interests of the counter disaster community as a whole.

These interconnected sites, are expected to become the building blocks for an integrated Australian Disaster Management Information Network (ADMIN). The initial emphasis of the project, however, is to provide support for local and regional activities, before considering broader applications.

Phase II: links to research and emergency networks

Provided that appropriate interconnection arrangements can be established, the next phase of the project will permit greater exchange of disaster-related information between the ADMIN network and other networks. Some inter-networking is already in place with FidoNet, a personal computer-based world-wide network of some 10,000 nodes. The results of other preliminary tests indicate that an electronic mail gateway to the Australian Academic Research Network (AARNet) and its links to over 100 research and educational networks world-wide through the Internet is also technically feasible, but requires further investigation into affiliation costs and agreements. Additionally, a gateway arrangement between the United Nations International Emergency Network (UNIENET) and the Internet has recently been initiated, allowing ADMIN users to automatically receive disaster situation reports from the United Nations Disaster Relief Office.

These combined arrangements, if successfully implemented, will electronically link disaster researchers, librarians and practitioners nationally and internationally, allowing access to up-to-date disaster-related information on a cost-effective basis.

Current status of project

ADMIX was officially placed on-line at the Australian Counter Disaster College on 19 June 1991. For the foreseeable future, access to ADMIX will be facilitated via dial-up telephone links, although other forms of data linking are also being investigated. Work by the project steering committee is focusing on a number of technical and operational management issues, including network planning and technical support, training, content development, promotion, organisational management and system security.

Role of ADMIN in disasters

Because of its present dependency upon land-line facilities, ADMIN is not intended to provide direct assistance during an actual emergency. Rather, its purpose is to support planning and preparedness for disasters. However, research is also underway to improve network integrity and security, as well as to assess the use of modified versions of the network software in disaster response and recovery operations. In particular, WICEN is assisting CIRCIT and others to develop and evaluate interconnection to these networks via digital radio.

Conclusion

There is no question that communication and information technologies play a critical role in the support of emergency operations. However, care must also be taken to ensure that the applications of CITs are not perceived merely as attempts to impose technical solutions on what are essentially human communication-related problems. Rather, they should be promoted as supplementary means to enhance information exchange and to appropriate new knowledge and skills for mitigating hazards, while at the same time recognising that organisational and user constraints may limit their effectiveness. Ultimately, the success of any CIT's implementation and potential long-term application cannot stand on its technical merits alone, but must be determined by the acceptance, usage of and relevance to those who participate in its use.

References

Anderson, P.S. 1990a, *Toward An Integrated Australian Disaster-Management Information System: Challenges and Prospects for the 1990s*, Policy Research Paper No. 4, Centre for International Research on Communication and Information Technology, South Melbourne.

Anderson, P.S. 1990b, 'Essential Services' in *Radio Spectrum Law and Management: proceedings of a CIRCIT Conference*, ed. D. Lindsay, South Melbourne.

Anderson, P.S. (ed.) 1991, *Proceedings of a National Workshop on Information Exchange Needs Assessment*, Centre for International Research on Communication and Information Technologies, South Melbourne.

Cochrane, H. 1991, 'Hazards Research is not Affecting Practice', *Natural Hazards Observer*, vol. XV, no. 6, pp. 1–2.

FLEET MANAGEMENT

William Horman
Director of Investigations
National Crime Authority
Former Commissioner
Tasmania Police
Secretary
Department of Police and
Emergency Services
Tasmania

The Budget Problem

FOR MOST LAW ENFORCEMENT AND EMERGENCY SERVICES AGENCIES, THE costs related to the purchasing, equipping, operating and maintaining of fleets is the largest single recurring cost, outside that of personnel. The cost of acquiring vehicles, the costs associated with equipping and maintaining these vehicles, and escalating fuel costs have created difficulties for many departments—including police. In 1991, it was announced that Victoria Police had taken a number of cost-cutting measures, which included requirements for detectives to leave their vehicles at the office and for general duties vehicles to spend time stationary whilst on patrol to reduce the use of fuel.

Faced with reduced or tighter budgets, which have resulted in ever-increasing operation constraints for departments, administrators are confronted with the need to minimise the cost associated with operating fleets. There are a number of measures which can be taken in an attempt to reduce costs and these include:

- selection of more fuel-efficient vehicles which are capable of meeting police operational needs;

- purchase of vehicles at the lowest possible price or utilisation of package deals;

- development and implementation of fleet maintenance programs to ensure all fleet vehicles are in peak operating condition; and

- development and/or use of driver training programs aimed at improving the efficiency of fleet operations.

The question of what types of vehicles should be used by police is an important one and in 1991, perhaps more so than in the past, departments are having to carefully consider the intended use of their vehicles and select the most suitable vehicle while taking into account cost factors. Purchasing overpowered vehicles and/or over-equipped vehicles is not cost-effective and not good fiscal management. Economic reality should cause administrators to accept some commonly known facts concerning the operation of most police vehicles:

- in urban areas, most driving is done at or below the speed limit;

- situations calling for urgent duty (pursuit) driving are comparatively rare in the total driving experience, and it has been suggested that pacing the suspect vehicle and effective use of communications are the key to a successful pursuit;

- most police vehicles appear to be normally occupied by one person;

- there has been a reduction in the size of communications and other equipment and, therefore, a reduction in the space required in the vehicle;

- the need for high speed capability in emergency situations is limited —and of questionable value in most cases.

Management Systems

It has already been mentioned that the vehicle fleet is a major consumer of police budgets, and fleet managers have come under increasing pressure to reduce costs and, at the same time, improve or at least maintain the level of service. Some factors which can be considered include:

- a standardised fleet: this means less cost for spare parts, training of personnel, special equipment and tools (where departments maintain their own vehicles); and

- a fleet management information system: designed to afford management reliable information on every aspect of the fleet service operation (thus enabling each vehicle to be monitored from the time it enters the fleet until it is sold or traded).

Police Crashes and Driver Training

One issue to be decided by administrators is whether or not there should be a hierarchy of classes of driving authorities issued to its staff; that is, whether an officer should have to qualify for a special 'in-house permit' in order to be authorised to drive certain types of vehicles, in addition to the officer's regular driving licence. The issue which follows on from this, then, is to decide whether or not driver training should be provided to officers to qualify them to drive particular types of vehicles and, if so, what form should this training take. After all, it is accepted that an organisation's administration is responsible, under health and safety principles, for its staff to be provided with adequate training to enable them to carry out required duties.

It is evident from media reports that police vehicles are involved in spectacular collisions. It is interesting that there appears to be no consensus of opinion or empirical proof as to whether or not driver training leads to a reduction in collisions. When the author was the Assistant Commissioner for Traffic in Victoria, Victoria Police's administration was concerned about the number and percentage of police fleet vehicles which had been involved in collisions. The initial figures were discouraging, but closer analysis suggested that it may not necessarily have been as bad as first seemed. For example, a comparison was made with vehicles of other emergency services and government and semi-government departments which concluded that the police figures were not so bad—in fact they compared very favourably if the analysis addressed other factors such as distance travelled. Yet something still had to be done to reduce these accidents, but what? Many of the incidents in which the vehicles were damaged were avoidable. Was training the answer, or at least one of the answers?

Examples of training

The Louisville Police Department (Kentucky, USA), after providing driver training for its officers, found that in the first six months after the training their overall fleet collision rate had been reduced by 40.2 per cent and collisions caused by officers had declined by 42.8 per cent (Auten 1982, p. 22). While the Daly City Police Department (California, USA) found that, after implementing such a training program, they were able to reduce the ratio of property damage to miles driven from .057 cents per mile to .017 cents per mile in just one year. The savings of .04 cents per mile resulted in considerable savings over the period of a year (Auten 1982, p. 22).

On the other hand, a study which examined the effectiveness of a comprehensive fleet management package applied to drivers of a large Melbourne Transport company, which included two post-licence driver training courses, concluded that:

- the overall package of measures was successful in reducing the drivers' accident involvement; but

- it was not possible to tell whether the package would have been successful without the training course (Manders 1986).

Concerns involving police vehicle collisions

Why the concern about traffic collisions involving police vehicles? What are some of the spin-offs?

- damage to the vehicles: huge repair bills, vehicle not available for work;
- injury and death of members: many man-hours lost; careers, health and lives often ruined; and three times as many Australians die through police use of vehicles than police use of firearms (McGrath 1991, p. vii)
- damage to police image and police/public relations;
- reduction in the efficiency and effectiveness of policing.

Aims of police driver training

Police training driver training should have three aims:

- training to reduce the likelihood of being involved in crashes;
- training drivers in fuel-efficient driving techniques; and
- ensuring that drivers have the correct attitude about their driving responsibilities.

Police Pursuits

Responding at high speed to what are often referred to as urgent duty calls was found by the National Police Research Unit (NPRU) to be:

> an entrenched part of the police culture [which] will be difficult to modify (McGrath 1991, p. vii).

Yet the NPRU went on to suggest a number of strategies which could be implemented:

- supervisors should be required to monitor and modify (where appropriate) the driving behaviour of those under their command;
- closer monitoring of police driving behaviour, supported by stepped monitoring through the command chain, would reinforce the message of driver and supervisor accountability (Risk Assessment Management Plan); and

- proposed national initiatives in police driver education should eventually lead to a change in police attitude towards urgent duty (pursuit) driving.

Factors which should not be overlooked when considering collisions involving police vehicles include:

- the age of the driver: in many cases the drivers of the vehicles involved in collisions are young officers with comparatively few years driving experience;

- all weather driving conditions;

- the driving environment and circumstances where the driver and other occupants are required to be especially observant of their surroundings for suspicious or criminal activities;

- the drivers of vehicles being pursued often intentionally crash into or cause police vehicles to crash.

Abuse of Vehicles

A disappointing aspect that seems to have been increasing in recent years is the abuse of vehicles. Often staff do not treat the vehicles with proper care, and it is not unusual to find fast food wrappers, remains of sandwiches, and empty cans or bottles in the vehicles, dirt on the dashboards where the passengers have been resting their feet, and a general condition that seems to indicate an attitude of 'who cares?'. This seems to reflect a number of issues, including a general lowering of supervision. Who is prepared to make 'on the spot inspections' and require some remedial action to be taken? How often are vehicles taken out on the road without any form of check? Who checks the pressure in the tyres? And what about the wheel nuts? Few drivers of departmental vehicles drive and treat the vehicles the way they do their personal vehicles. Why? And what is being done, or can be done about it?

What has to be remembered is that poor maintenance, lack of vehicle checks and abuse can result in reduced safety for the officers. How often are vehicles thoroughly checked by officers concluding duties or just about to commence? What about syringes, knives or other weapons which could be tucked down behind the seats?

Another aspect of vehicle abuse which adds considerably to departmental costs is the private use of departmental vehicles. Fortunately, this issue has started to be addressed in recent years. In some situations, jobs have been identified as entitling the Senior Executive Service (SES) officer to have a vehicle for personal use which, in some instances, is included in the officer's overall salary package. Police departments should require all vehicles, other than those especially exempted on defined criteria, to be clearly marked as 'police' vehicles. This can have a number of positive results including:

- greater police visibility on the roads resulting in a number of positive spin-offs;
- increased onus on the driver to drive more responsibly and treat the vehicle in a more appropriate manner; and
- less likelihood of private abuse of the vehicles.

The police administrator, today and in the future, is going to be very accountable for the management of the department's fleet and will need to ensure that maximum efficiency is obtained from the fleet budget vote. Change will be necessary to achieve this efficiency and savings in productivity, and this will require recognition of the importance of management and marketing to personnel of the role they—and every vehicle user in the department—will have to play to help achieve department goals.

Bibliography

Auten, J.H. 1982, 'Police Fleet Considerations', *Law and Order*, vol. 30, no. 11, November, pp. 21–3 ff. 66–7.

Brown, R.L. & Cofer, T.E. 1979, 'The Missouri State Highway Patrol Fleet Program', *The Police Chief*, vol. XLVI, no. 12, December, pp. 38–9.

Chalkley, M.T. 1980, 'A Case for Computerised Fleet Management', *Law and Order*, vol. 28, no. 11, November, pp. 60–2.

Dolce, J. 1984, *Fleet Management*, McGraw-Hill, New York.

Donnelly, H.A. 1985, 'A Management Information System for Fleet Service', *The Police Chief*, vol. LII, no. 9, September, pp. 29–31.

McGrath, G. 1991, *Urgent Duty Driving by Australian Police: Facts and Recommendations*, National Police Research Unit, Adelaide.

Manders, S. 1986, *Fleet Management Techniques: An Investigation of the Effectiveness of Various Techniques on Vehicle Collision Prevention*, Road Traffic Authority, Hawthorn, Victoria.

A NATIONAL POLICE CAR?

Warren Hill
Fleet Management Services
New South Wales Police Service

PRIOR TO 1978, THE NEW SOUTH WALES POLICE SERVICE HAD CONTEMplated the possibility of a car which had been exclusively designed and equipped for at least general police duties. The considerations of an exclusive vehicle were prompted by the difficulties and frustrations then experienced with police use of what were standard production family type sedans, for example:

- the carriage of prisoners;
- speedometer unable to accurately define the actual extent of speeding offences;
- electrical/battery failures due to the amount of police equipment;
- sub-standard performance for high speed pursuits;
- braking systems and suspensions inadequate for regular higher speed use;
- engines overheating due to long periods of idling at scenes of emergencies;
- non-ergonomic seating, unsuitable for a full police duty shift; and
- regular seat frame failures due to the physique of police.

The time and expense of converting a standard vehicle for police purposes was a further factor in the exclusive vehicle consideration; for example, purchase, maintenance and installation of accurate speedometers, rewiring to accommodate police equipment, and purchase of heavy duty batteries.

The New South Wales Police Service was aware of the European availability of specially built 'Police' Volvo and Mercedes-Benz sedans, and also the 'black and white' sedans used in parts of the United States of America.

Vehicle Requirements

The characteristics and specifications of a national police car will, of course, be decided by the vehicle needs and expectations of each Australian police force. Briefly, and using New South Wales as a guide, duty demands of the national vehicle would include:

Transportation of police service personnel

It is usual for the majority of general duty vehicles to have a crew of two, as do highway patrol (pursuit) vehicles on afternoon and night shifts. The larger stations in New South Wales are 'on the job' training locations and a 'student' police officer accompanies the general duty crews.

Transportation of prisoners

In New South Wales, the carriage of prisoners in sedan vehicles is minimal. Nonetheless, it is essential that prisoners in sedans are transported securely and safely, and without exposing escorting police to violence or driver distraction.

Transportation of equipment

The duties of most speciality units dictate the carriage of bulky items:

- dogs;
- breath analysis equipment;
- forensic evidence equipment such as cameras, fingerprints, plaster casts, and measuring devices;
- portable generators;
- small refrigerators for exhibits;
- exhibits found at crime scenes;
- bullet-proof vests;
- police warning signs, witches hats, and similar traffic control items; and
- typewriters, forms, stationery.

The carriage of this equipment necessitates the use of station sedan vehicles.

General duties — metropolitan centres

Vehicles used in city suburban areas normally travel in the speed band of 30–65 kilometres per hour. Good acceleration in the 50–90 kilometres per hour range is required, and a top speed in the vicinity of 150 kilometres per hour is sufficient. Improved vehicle handling and stability are genuine aids to safe manoeuvrability in congested areas.

General duties — country centres

Duties in country centres are similar to the requirements for the city vehicle, with the additional needs of:

- long-range fuel tanks in recognition of Australian outback distances;
- a suspension and other under-car fittings of sufficient strength to combat the poor road conditions in outback Australia;
- improved vehicle handling in view of the poor conditions and when operating in areas subject to snow, ice or high rainfall;
- sufficient ground clearance; and
- sufficient towing capacity.

Highway patrol (pursuit) duties

Capable of cruising at 80–110 kilometres per hour for sustained periods, with a rapid acceleration ability, especially in the 80–160 kilometres per hour range. A top speed of around 210 kilometres per hour. A high speed suspension, limited slip differential, and long-range fuel tanks are essential.

Plain clothes (detective) duties

A vehicle appearance which does not readily identify with police use and with a performance ability similar to that of the general duty vehicle at metropolitan centres.

Surveillance/undercover duties

A vehicle which blends in with surrounds and which does not disclose the officers' true identity in any way. Sufficient performance so as to closely follow any other vehicle in traffic, and an appearance and equipment level which suggests comfortable means in cases such as undercover drug dealings. An interior which allows 'covert' fitting of radios and other police equipment.

Administrative and welfare

A vehicle which is not readily identifiable with the police service, and with performance sufficient for comfortable/legal city and country travel.

Executive

A vehicle which does not readily relate to the police service, and with the performance and equipment levels normally associated with company managers. An interior which allows 'covert' fittings of radios and other police equipment.

Characteristics of a National Police Car

To cater for the various duties of police, for the differing terrains and climates experienced in Australia, and for the requirements of all Australian Police forces, it would be necessary for a national police car to be available in a number of versions and with a number of engine options. The specifications for the specially-built vehicle would include:

- the capacity to comfortably accommodate at least three police;
- the capacity to securely transport at least two prisoners, with ease of access;
- an interior designed to accommodate the standard police speciality items, for example, radios, radar units, on-board computers, telephones, batons, torches, and similar items;
- an interior with the latest safety features of heavy padding, air-bags and, of course, strong seat belts;
- ergonomic design seating, cloth covered with hard wearing material, lumbar supports, lateral and height adjustment, and sufficient frame strength to accommodate police use;
- the option to fit full interior crash-bar equipment to highway patrol sedans;
- the interior must conform to Australian design rule standards and enable compliance with occupational health and safety obligations;
- a capacity to securely carry the equipment necessary for certain duties; for example, breath analysis equipment, rescue equipment such as metal cutting axes and pinch bars, fingerprinting equipment, cameras, shotguns and other heavy weapons, accident investigation equipment, and police dogs;

- an engine performance suitable for general duties in metropolitan and outback centres, for plain clothes duties, administrative and welfare, surveillance and undercover, executive, and highway patrol (pursuit) duties;

- a comfortable ride, handling capacity consistent with engine performance and suspension hardy enough to cope with the harsh conditions of outback Australia;

- a braking capacity which is more than adequate to the engine performance, especially for pursuit sedans;

- wheels and tyres adequate to engine and handling performance;

- an electrical system to allow for the standard police speciality items, which will not cause electronic interference to those items;

- long-range fuel tanks to cater for the distances of outback Australia;

- heavy-duty batteries;

- power steering;

- a mechanical technology prescribing longevity, reliability and minimum maintenance;

- a modern aerodynamic exterior, capable of accommodating flashing lights, sirens, public address systems (usually roof-bar mounted) and police decals;

- full instrumentation, with the availability of an incremented and calibrated speedometer suited to the accurate detection of speeding offences, to the satisfaction of courts;

- a range of acceptable external paint colours so as to promote vehicle individuality as far as possible; and

- a range of options such as limited slip differentials, engine sump and transmission protection kits, air conditioning, heating, tow bars, bull bars, headlight and front of car protectors, high speed rated radial construction tyres, luxury appointments, and independent rear suspension.

Practicality of a National Police Car

In any discussions as to vehicle availability in Australia, it must be remembered that the Australian market represents less then 1 per cent of the world trade. The demands and expectations of a national vehicle are varied, and these factors would no doubt multiply as all requirements of all Australian states were defined and recognised.

It is considered that the outright design of a new and exclusive police vehicle, and the associated implementation of construction/assembly production lines, would be cost-prohibitive to the extreme, and a resident manufacturer would not be receptive to such a proposal due to:

- the intentions and strategies of (overseas) parent companies in regard to local operations and future vehicle models;
- the local long-term planning and commitments in support of these strategies;
- the policy of government to stabilise the number of available vehicle makes and models;
- the necessity to divert significant time and resources to the exclusive car project—to the detriment of the activities which constitute present and future profitability—and a continued high profile presence in Australian manufacturing;
- the limitations of construction/assembly production lines; and
- the small market for the exclusive vehicle.

Whilst the use of an overseas exclusive vehicle may be possible, there are a number of disadvantages to this course:

- the cost of modifying existing vehicles to comply with Australian vehicle regulations (for example, right-hand drive, emission gas standards and controls, the construction and layouts of dashboards);
- the manufacturer offering the vehicle on an 'as is basis' and being unable or unwilling to recognise requirements unique to Australian police forces;
- the costs, delays and inconvenience of importing vehicles;
- the ability of the manufacturer to support the vehicle in terms of maintenance, repairs, and parts on an Australia-wide basis;
- the attitudes of Australian governments towards the importation of the exclusive vehicle;
- objections from resident manufacturers; and
- limited resale attraction of an overseas 'special' vehicle.

It is considered that the only genuine opportunity for a national police car which completely satisfies all requirements is by way of a resident manufacturer further altering the build techniques and design of an existing production vehicle. Unfortunately, this option is not without unfavourable circumstances, detailed as follows.

Additional costs

The further modification of an existing Australian vehicle would not, of course, be without additional costs. Extra public expense is, naturally, contrary to the policies of all Australian governments for the foreseeable future. Approval of additional funds

would be dependent on commensurate savings being effected elsewhere in vehicle spending.

The most obvious means of effecting savings is by reducing vehicle numbers, which is not likely to be acceptable to the Australian police forces.

Extended vehicle retentions

Extended vehicle retentions are another measure often suggested as cost-effective. Australian police forces generally dispose of sedan vehicles around two-years-old or when they have travelled 40,000 kilometres. The reason for this policy is that resale losses are minimised by disposal when the vehicles are still the current models and with relatively low kilometres recorded. It is also considered that the vehicles are sold before expensive overhauls of major components are necessary, and before manufacturers' warranties expire.

Studies in New South Wales—where sedan vehicles are usually sold when less than twelve months old—have confirmed the logic of the above disposal policy. The suggestion that extended vehicle retentions would be another avenue of effecting measurable savings appears to be a false premise. Indeed, costs may actually escalate:

- maintenance and repair expenses must substantially increase with increased kilometres and prolonged use, especially after the expiry of manufacturers' warranties;

- resale prices will significantly decrease with increased kilometres and disposal age; and

- a larger capital outlay would be necessary to replace an aging fleet.

Restricted purchasing of vehicle makes and models

Other than costs and specific clauses of government contracts, there are no limitations on the makes and models of vehicles which the New South Wales Police Service can purchase for Surveillance/Undercover, Administrative and Welfare and Executive purposes. This flexibility could be greatly curtailed or even eliminated with the introduction of a further altered production vehicle in an endeavour to increase the market for the vehicle and thereby reduce costs.

Reduced resale prices

A restricted mix of vehicle makes and models offered for sale would reduce the overall annual resale figure. The sale of vehicles which are perceived to be too 'exclusively police' would also lower resale prices.

It there Already a National Police Car?

Prior to 1978, there was no alternative for the Australian police forces but to purchase whatever available standard production vehicles best suited their requirements. Any modifications were an individual 'after market' arrangement.

In 1978, representatives of the Ford Motor Company of Australia approached the New South Wales Police Service with an offer to build a 'Police Special' sedan. Consultation with each of the other Australian police forces soon followed. Eventually, the forces were able to agree upon what fittings and modifications should be standard items in the 'Police Special'. The 'Police Special' entered production in 1978 and materialised in the form of the 'Falcon' family size, six, or eight cylinder sedan. General Motors–Holden introduced a similar option in the 'Commodore' sedan around 1981. The vehicle enhancements form what is now known as the *Police Pack*, which consists of:

- an upgraded suspension suitable to high speed driving;
- 15 inch steel wheels;
- high speed rated tyres;
- a heavy duty all wheel disc braking system;
- an electrical/electronic system specially modulated so as not to cause interference to police radios and other speciality items, and a system which conversely cannot be affected by the police items;
- increased alternator output so as to accommodate the use of the police speciality items; allied with a large heavy duty battery;
- battery couplings for the connection of police speciality items;
- apertures in the firewall and in the rear seat housing to allow installation of cabling for police speciality items;
- manually-operated map reading lights, and disconnection of the automatic door courtesy lights;
- map pockets;
- full dashboard instrumentation;

- an incremented speedometer, which is calibrated to the accurate detection of speeding offences to the satisfaction of courts;
- additional automatic transmission oil cooler;
- removal of the transmission 'gate' between drive and second gears, to facilitate quick gear selection at speed;
- individual and ergonomic design front reclining seats, with lumbar support, and lateral and height adjustments on the driver's seat;
- separation of the front seats by a full length console which incorporates a floor mounted 'T-bar' gear shift;
- a long-range fuel tank allowing a minimum driving range of 450 kilometres;
- an optional V8-configured engine of around five litres capacity and an optional limited slip differential for pursuit vehicles; and
- optional air conditioning.

Virtually all Ford Falcon and Holden Commodore sedans purchased by the New South Wales Police Service are fitted with the *Police Pack*. The enhancements have proved most successful in New South Wales and there is universal recognition and appreciation of the benefits.

The standard *Police Pack* is reasonably priced at under $A1000 per unit and both Ford Australia and General Motors–Holden regularly consult the New South Wales Police Service as to the suitability of the *Police Pack*. The manufacturers convene a conference of representatives of each Australian police force if the *Police Pack* will be affected by major vehicle model changes.

Conclusion

- The *Police Pack* equipped Ford Falcon and Holden Commodore sedans already constitute a national police car.
- Each Australian police force has ample opportunity to request improvement of the *Police Pack* to suit any additional needs.
- The *Police Pack* is comparatively inexpensive and has proved successful.
- The *Police Pack* equipped sedans are suited to general duties, pursuit duties and plain clothes duties.
- An acceptable range of colours, options and engines—and station sedan versions for equipment carrying—are available.

- The *Police Pack* equipped vehicles have a good resale attraction.

- The availability of the *Police Pack* equipped sedans does not restrict flexibility in the choice of vehicles for Administrative and Welfare, Surveillance/Undercover, or Executive purposes.

- While the *Police Pack* equipped vehicles do not incorporate all possible items, the Australian economic climate precludes the immediate need for an exclusively designed and built ideal national police car.

SECURITY OF PUBLIC PLACES: AN OVERVIEW

Graham Bourman
National Marketing Manager
Australian Protective Service
Victoria

THE EMPHASIS OF THIS PAPER WILL BE ON THE PROTECTIVE SECURITY OF assets and installations in which the federal or a state government has an interest. This accords with the broad charter of the Australian Protective Service (APS).

It is obviously no revelation to state that the financial screws are being tightened to shear-point, and security and law enforcement agencies could be asked (or told) to show further savings—probably without visibly reducing service levels and risking criticism from the people we serve. However, to be pragmatic about the situation and to get on with the job professionally, all measures which show enhanced cost-effectiveness without prejudice to operational effectiveness have been sought. These measures include the time-honoured reorganisation of security and law enforcement agencies in order to demonstrate savings. However, the reorganisation process is more attuned to activity rather than productivity. There is merit in staff reorganisation but, unless there are dramatic inefficiencies to be overcome, the resultant disruption to operational patterns and the lowering of the morale of members who resist change can have a detrimental effect on cost-effectiveness—at least in the short term.

Historically, human resources were thrown at any problem with the full expectation that the problem would be solved. This type of usage of human resources is no longer affordable and more cost-effective options are required. The age of technology is here, and will probably remain forever. The correct use of technology, the correct mix of technology and people, and the vision to look a very long way 'down the track' to ensure the money expended today will provide the expected and required solutions in the future are vital aspects of any security program.

Having arrived at the conclusion that a crystal ball with adequate software is needed to give expertise in people/technology mixing, security law enforcement agencies are then faced with the plethora of technology available. Most people are not technicians, and indeed, most people—even those with a sound knowledge of available technology—probably cannot decipher the varied and complex responses to the question: 'How does this technology work?'. User-friendly technology is required.

This paper will briefly recount the genesis of Commonwealth protective security leading to the activities of the Australian Protective Service as it operates in public places in 1991 and its use of technology—including a vision of the future.

Commonwealth Protective Security

During World War I—probably as a response to the internment of 'aliens' in Australia—the Commonwealth Police was formed and performed protective security duties by rounding up aliens and holding them in internment camps. Additionally, the Commonwealth Police guarded vital establishments. At the end of World War I, the Commonwealth Police Force was disbanded and the Peace Officer Guard was formed to continue the guarding function. The Commonwealth Police Force was eventually reformed, absorbed the Peace Officer Guard, and in the late–1970s became the Australian Federal Police (AFP), having narrowly missed becoming the Australia Police. The AFP had two components: the *general duties* policing component, and the *protective services* component which in 1984 was transferred to the federal Department of Administrative Services to form the nucleus of the newly formed Australian Protective Service (APS).

The APS started life as a budget-funded component of the large Department of Administrative Services and spent its formative years coming to grips with the dichotomy of having a uniformed, armed, and disciplined service composed of public servants employed under the *Public Service Act* and subject to the Public Service Regulations. Teething problems were inevitable as the APS found its feet, generated its culture, and focussed on providing a service to its clients in consultation with them.

For the first time, clients were asked to enter into a form of contract with their security providers. Memorandums of Understanding (MOUs) were prepared for each client and showed the services to be provided, staff levels and other details. In 1991, the APS receives no direct government funding and all revenue is received from clients who, with rare exception, are free to seek alternative service providers.

The history of Commonwealth security forces has, therefore, seen many changes and, in 1991, the APS is in the best-ever position to be an effective service which will rise or fall on its own merit. This commercialisation has been very challenging as it has focussed attention on providing cost-effective services in response to specific client requirements—the APS does not merely fill rosters with little emphasis on accountability or costs. This commercialisation of services is a vital and necessary process which has propelled the public service headlong into the realities of working both for the client and in their interests.

Public Places

There is no easy definition of a public place—it encompasses extremely diverse areas. The onus is on every landlord, employer, and manager to provide a safe and secure workplace. Add to this the specific need for some businesses to protect the assets of the Commonwealth or state, national secrets, information provided by foreign governments in areas of cooperation such as defence research and communications, and Internationally Protected Persons, and the security net widens substantially requiring very flexible and responsive service providers. The security of public places, therefore, covers many requirements.

Historically, human resources were used to cover all requirements. The more sensitive the area, the more human resources were deployed to protect it. This is still germane in 1991, but to a far lesser extent as cost pressures force the need to exploit other options and to reassess the basic need for security at every installation. The 'old' days of 'meeters and greeters'—convenience gates opened for staff who did not accept the additional walking or driving, or the perceived importance of an establishment deciding the high numbers of security personnel on duty—have either gone forever or are about to be removed from the last of the establishments now coming to grips with the realities of their reducing budgets. To give examples of these areas the following illustrates the client base of the APS:

- category 'one' and 'two' airports, where the APS provides a counter-terrorist first-response force;
- joint defence facilities at Pine Gap, Exmouth, and Nurungar;
- immigration detention centres;
- defence research establishments;
- diplomatic and consular protection;
- the new Commonwealth Parliament House;
- access control of 'sensitive' Commonwealth agencies;
- any other areas demonstrating a 'Commonwealth interest'. These can be state government or commercial clients; and
- security advice and training services.

The clients cited vary in type from comfortable offices in Australian capital cities to the desert of Central Australia, and the remoteness of north-west Australia. The duties vary from being very authoritarian to being very understanding of other peoples' problems and demonstrating very high interpersonal skills—as is essential at immigration detention centres, where people of most nationalities (males, females, and children) are held pending a court decision on their status as an Australian citizen. Thus, the definition of a 'public place', in this context, is extremely broad. The unchanging element is APS accountability for providing quality services.

The effect of commercialisation has seen some APS clients put their requirements to open tender and the APS not regain their business. Some areas, particularly areas where access and egress control in basic office areas was the sole requirement, accepted the services of the lowest priced tender and switched to commercial services. The APS did not see this as an indication of a lack of faith in its abilities, but rather as a natural concomitant of financial constraints in the 1990s. The managements of these public places practised risk management by reducing the quality, and hence the cost, of their security and accept this reduced service as 'adequate'. The APS offered only one level of service—the highest. Not all clients need an expensive service level. The benefit to the APS of this experience is that it now has a 'second tier' service to offer clients. The APS has officers who are not trained to the original, all-encompassing high standards, are not paid to the same levels, and, consequently, their services are commercially competitive in price. The APS does, of course, maintain its original service tier for those areas which require it. As a result of recent client losses, the APS offered voluntary redundancy to 150 officers nationally. Although the APS is not striving for maximised staff numbers, it is likely that the second tier service will more than recover the 150 staff losses.

To summarise, public places covers such a wide variety of security requirements that each threat and risk assessment sees a mix of solutions (both human and technological) being used. The quality and cost of these solutions is determined by the perceived importance of the particular public place.

Technology

Technology can save money and be more cost-effective, OR, technology can be expensive, complicated, unreliable, and put one at the financial mercy of technicians. Both these statements can be true depending on the wisdom of the technology selector or the quality of the advice given to that person.

There is an absolute plethora of technological devices on the security market in 1991. One can buy devices to open safes, close safes, delay safes from opening. One can buy biometric devices which read eyes, palms, and fingerprints. The Japanese have a computerised device which can read the shape of one's facial features to a very high accuracy in spite of attempts to mask one's appearance. Intruder alarms can do nearly everything, including make the coffee at the appointed time. Access controls use a wide variety of technology, most involving a plastic card or key (which does not necessarily belong to the user). The only guidance for technology selection the APS has is that the technology must do the job for which it is selected, must do that job reliably, and must be cost-effective. The starting point for determining which technology to purchase, therefore, is always to carry out a thorough threat and risk assessment and only select technology which satisfies the set requirements. Risk management by adequate insurance cover may alleviate the need for security in some areas and this option is not always available to government areas—choosing technology can be a confusing and sometimes frustrating experience.

Technology in protective security is cost-effective and is the way to go, but technology must be very carefully selected and only after it has been seen to operate effectively in a similar situation to that required. The APS has a stated aim of using technology where it can be demonstrated to be more efficient or more cost-effective. The APS does not intend to advocate technology for technology's sake and the individual client's needs will always determine which parameter drives the decision.

The APS has invested substantial time and money in developing its technological awareness and expertise. The APS has, for example:

- in 1990, sent two senior officers to Singapore to study protective security in that country. The officers visited organisations such as the Commercial and Industrial Security Organisation (CISCO), the Singapore Police, the Singapore Air Terminal Services Security Organisation (SATS Security Services), the Singapore Port Authority, and a commercial organisation. This visit was found to be a valuable learning process and it was concluded that Australia is in the forefront of both effective security services and the use of technology;

- held a Certificate of Technology course, through the Latrobe University, where the APS qualified a broad range of its officers to this standard. More officers are currently on a similar course being held for TELECOM;

- sponsored financial reimbursement of fees and purchase of textbooks for APS officers undergoing the Associate Diploma of Security Management course at the Phillip Institute of Technology. In Victoria, four officers have graduated from this course;

- entered into joint agreements with commercial companies who are developing leading-edge technology and has assisted them with marketing and promotion of their products;

- a policy of promoting Australian developed and manufactured technology ventures wherever it can. Obviously the APS is discriminating and believes the products it promotes have sound merit. An example is the use of Zone Technology Digital CCTV systems which transmit television pictures through a dedicated or dialler telephone line to APS Central Stations in Canberra and Melbourne. One technology is 3DIS, a three dimensional interactive-space alarm system which uses CCTV cameras, through a personal computer and dedicated software, to provide active freestanding alarm zones which can be drawn, and redrawn around any object or area by the personal computer's mouse. A sixteen camera installation is currently successfully guarding stabled trains from graffiti vandals in Melbourne;

- developed two Central Stations; one each in Melbourne and Canberra. These stations will be certified to National Grade One standard by the end of 1991 and monitor dialler and direct line alarms; and

- a dedicated technology officer in the National Office who maintains focus on technological developments and gives advice to regions.

This level of commitment is felt to be necessary if the APS is to provide quality services to public places.

The Future

The future will see far greater acceptance and use of technology in many areas. One has seen the explosion of technology in the information arena; for example, in our homes with video cassette recorders, compact discs, clocks that 'talk'; and in children's rapid acceptance and need for personal computers. Some of the areas security is likely to enter in the future are:

- fully-automated electronic security systems with no human component at the operating level. These systems would provide the necessary controls—be it access/egress control, building opening or closing, or security of assets. All infringements would be automatically reported to a computer program which, drawing on its various databases, would verify the infringement, identify the person or persons responsible, allocate a penalty, and take the necessary corrective action;

- vehicle tracking systems which will remotely display a vehicle's position on a computerised map. Satellite communications would extend the currently available city-based systems to all areas of Australia;

- biometric systems which use DNA analysis to provide identification of people, with no errors;

- perhaps an 'electronic policeman', fitted to every vehicle, which notes the traffic infringements of the driver, transmits this to a centralised police computer which electronically deducts the appropriate penalty from the vehicle owner's bank account and sends out a Traffic Infringement Notice with a receipt attached; and

- remote electronic tracking of people (children) through micro-chip implants. This system is currently used to identify animals, albeit not remotely.

Conclusion

Technology and its uses are limited only by imagination and finances. In the security of public places arena, technology is consolidating its position as a cost-effective alternative to human resources and is positioned to make further inroads in that direction as reliability and cost factors improve. Given the choice between technology and human security, the human factor would always be preferred. Properly trained, managed, and equipped, the security officer can decide a course of action by logically

assessing factors which have not necessarily been pre-programmed or envisaged, can be relied on to act even if not 100 per cent serviceable, and can offer advice based on experience. In the future, the choice of human resources may not be affordable.

TECHNOLOGY AND THE PRIVATE SECURITY INDUSTRY

John Hemsley
Corporate Security Manager
Davids Holdings Pty Ltd
Sydney
New South Wales

A General Overview of the Private Security Industry in Australia

SECURITY COMPANIES AROUND AUSTRALIA HAVE FOUND A NICHE AND provide private security services that the federal and state police forces cannot provide because of personnel levels, increased serious crime and to a lesser extent, the lower priority of private security services as far as the police are concerned.

The overall growth of the Private Security Industry (PSI) has increased at an unprecedented rate during the 1980s. Probably the best example of this is in New South Wales, where the Sydney security section of the telephone directory has increased from two pages in 1985, to over twenty-eight pages in 1991. New companies have been formed overnight and their services cover the total gambit of security services. This has lead to increased competition in the PSI, but the main feature that emerged from this competition was the formation of three distinct levels of service providers. These service levels are: firstly, the major contractors dealing with projects and government-type contracts; secondly, the medium-size companies who deal primarily with the commercial sector; and thirdly, the one-man businesses dealing with domestic services.

Enter the *Security Protection Industry Act 1986* (NSW)—the first attempt to regulate the PSI by setting standards and protecting the end users. The result of the implementation of this legislation is that, after several years in operation, retired magistrate Reginald Bartly recommended that the Act be withdrawn. In 1991, the situation is that the Act is still in force, and no-one pays it any attention. This highlights the complete inability of the PSI and the state governments to work together and form a self-regulating, government-overseeing PSI where the standard of all services are set to protect the end user.

To visualise the extent of the PSI consider the combined turnovers of the national players who include: Mayne Nickless (MSS Guards, MSS Patrols, MSS Alarms, Armguard), TNT, Wormalds, Honeywell, ADT, Chubb, and Racall. These companies are providers and do not include self-providers such as the Electric Authority, Water

Board, Coles, Woolworths, Myers and many others. Add to these the medium and small companies, and it can be seen that the PSI in Australia is enormous, unregulated and has a high dollar turnover.

The Need for Facilities and Services provided by the Private Security Industry

The crime rate in Australia is increasing in almost all areas, and the ability to fight that increase is diminished because of the current financial restraints placed upon the law enforcement agencies and the community in general.

Priorities are set by the enforcement agencies and, because of these restraints, an attitude of these agencies has begun to emerge, being that in times of increasing demand on the enforcement agencies' time, priority will be given to those who help themselves in the community at large. In other words, the companies that show a proactive approach to crime rather than a reactive approach will receive first assistance from the police. An extreme example of this would be of two companies both with loss prevention problems: the first a retail store setting out its produce for maximum exposure to prospective purchasers with the policy of catching an increasing number of shop thefts as they leave the store. The second retailer sets out his products with the policy of loss prevention in mind. This scenario must be tempered with a fair degree of commonsense and the ability to arrive at a balance, for if the products were locked away there would be no loss, but also no sales. It is obvious which company will drive the police mad first.

To those national companies dealing with the police on almost a day-to-day basis, the trend has been evident for some time. This, together with a genuine interest in becoming self-sufficient in the reduction of unknown losses and other crimes against the company, has created the need for in-house security and services supplied by the PSI.

The four groups that are connected with the PSI are:

- contractors;
- self-providers and users;
- consumers of the services; and
- equipment suppliers/manufacturers.

Some of the services supplied by these groups include:

- access control systems;
- alarm equipment manufacturers/wholesalers;

- armoured car services;
- commercial/industrial alarm installers;
- home alarm installers;
- car alarm installers;
- 24–hour monitoring services;
- 24–hour central station operators;
- fire alarm manufacturers/wholesalers;
- fire alarm installers;
- security guard services (static guards and mobile guard mobile/foot);
- locksmith services;
- safes and record protection;
- closed-circuit television systems;
- security grills, fences and doors;
- alarm responses; and
- investigation private/commercial inquiry.

There are other reasons that private security services are used, including the following:

- there are groups of people who have recognised the need to take precautions to protect their homes, family, business premises and stock against crime;
- there are those who are using the services of the PSI because insurance companies will not issue or renew a policy without some security, possibly because of past history of losses or damage; and
- there are some people that install an alarm system so they can claim reduced insurance premiums.

It does not matter for what reason private security services are used, the end result is that, if these services are used and used correctly, the community in general will benefit by reduced costs.

Technology and the Private Security Industry

Technology, as defined in the Macquarie Dictionary, is:

> the branch of knowledge that deals with science and engineering or its practice as applied to industry.

Technology in the PSI can be separated into two main sections: physical and electronic protection. This paper will deal with the electronic side of security, as the technology of the physical side is a complete topic in itself.

Electronic alarm systems

Electronic alarm systems fall into two basic categories: local alarms, and monitored alarm systems. Both can be silent or have a siren and strobe fitted.

Local alarms: The most common local electronic alarm system relies on the good nature of the general public to respond. Even though the detectors may be the same as used in a monitored system, the signalling or communication media leaves much to be desired. An extreme example of this could be a local alarm system fitted to a home. It is a cold and stormy night in the middle of winter and the alarm on the house over the road goes off. Would you get up and investigate? No. Neither would most people. So it can be seen that in the case of a local alarm activating, it may or may not receive a response.

Monitored alarm systems: The main feature of a monitored system is that a person somewhere—either on site or at a remote base—is monitoring the alarm activation and will respond in a predetermined manner to an alarm. This ensures a response and, hopefully, a minimum of losses, or the summoning of assistance in the case of physical threats, or the supplying of medical assistance. There are several acceptable types of monitored alarm systems, listed in order from that offering the highest degree of security to that offering the least: Direct line; R.F; Securitel/alias function dialler; and Dialler.

Various methods of detection

Passive Infra-Red Detectors (PIRs): These are the most common detectors and are designed to pick up electromagnetic radiation which is emitted by any object at any temperature above absolute zero. The actual amount emitted and the wavelength produced depend on the temperature of the object and its emissivity. The advantages of PIRs are:

- they are simple to install;
- there is no penetration through glass;
- units do not interact with each other;
- rattling or vibrating items do not activate it;

- advanced sensors and microprocessors make them reliable; and
- hot and cold air streams do not affect them.

The disadvantages of PIRs are that they are subject to false alarms if installed over a refrigeration unit or heater that causes a rapid change in temperature.

Microwave Unit: This detector has been used for years. The advent of solid state microwave components has made the use of this device economical. The microwave operates using the Doppler Effect. When a moving object comes into the field under surveillance, the reflected signal from that moving object will give a slightly different frequency from the transmitted signal so triggering the detector. Disadvantages are that care must be taken when microwave units are installed as this detector can see through walls, glass and pipes and will react to running water as it passes through the pipes.

Photo Electric Beams: To activate this device, an object must pass through the beam that is transmitted from the transmitter to the receiver. This is a very effective method of detection and is not prone to false alarms. In some circumstances where there are problems with birds or other animals, two photo electric beams are used and to be activated require both of them to have their beams broken.

As problems exist with both Microwave and the PIR, a unique way of eliminating those problems is to combine the two technologies to form a Dual Tec or Double Tec. This unit requires both body heat and movement at the same instant to generate an alarm thus eliminating a lot of unwanted false alarms and allowing the unit to be placed in most environmentally unstable areas.

Closed Circuit Television (CCTV): Technology in the CCTV areas has advanced and is still advancing at a rapid rate. The camera is no longer just black and white, colour has produced extraordinary results. Videcom Tubes have been replaced by the closed circuit camera, where images are formed by microprocessors inside the camera and can work in low light—as low as 0.2 of a lux, which is the equivalent of standard street lighting. There are colour cameras that are remarkably compact, and pinhole cameras for covert operations which are virtually undetectable.

Technology has developed a method to photograph people or objects from close range to a vast distance by telephone. This involves the camera being activated by a device taking a picture and transporting that picture down a phone line to a receiver where the picture is upgraded, placed into a monitor and then printed on medical grade paper to give a perfect image. Imagine a car yard with photo electric beams protecting the perimeter of the showroom. The alarm is activated and the client is contacted and notified of the alarm condition by the monitoring control room. With the technology discussed above the client no longer needs to attend the site to establish the reason for the activation, the camera will automatically take a photo of the offending section and the client only need be contacted if the situation demands a response.

Even the need for a phone line is eliminated by the use of microwave links. These links are repeater stations which carry the image in wave formation to its destination—to the receiver where it is again processed by the control room and a

photo image obtained. These pictures can be faxed to the relevant police station to assist officers in identifying offenders at the scene of the crime.

This technology can also be used in reverse; that is, the receiver controlling the cameras. A person can dial the corresponding security code of a premises and select a particular camera, turn it on and obtain a photo at the base. A manager could check on the night shift staff at his factory from his house with this system. Many companies that are charged with the total building management will have a similar system looking at the various gauges in the plant room for better control of the building.

This technology has unlimited boundaries. In the future pictures will be sent by hand-held phones via satellite to their destination.

Industry Standards and Associations

There are numerous associations and institutes throughout Australia, some state-based, others with national affiliations, some representing major contractors, others representing smaller companies. During the past few years there has been a call to combine the various associations from both within the PSI and from some state departments. There was a call for the PSI to speak with one voice, but this was unrealistic and, on reflection, undesirable. As the PSI is still so young and growing so rapidly, one association could not hope to effectively service the total industry. The overall aims of all the PSI associations seem to be similar. This paper will only examine one—the one that controls the largest percentage of security dollars—the Australian Security Industry Association Limited (ASIAL).

Australian Security Industry Association Limited (ASIAL)

Consumers tend to use members of these organisations because of their accountability. For example, ASIAL members must supply all services and equipment to conform to the relevant Australian Standard. This gives protection similar to the Motor Traders Association in New South Wales. Further insight into ASIAL can be seen by looking at its aims:

- to promote and foster amongst persons, firms and corporations engaged in the Australian security industry the highest standards of efficiency, service, equipment, and ethical behaviour;

- to give the utmost cooperation to the police forces of the Commonwealth and various states of Australia and other lawful authorities for the prevention of crime;

- to do things necessary and lawful to ensure that there is always available to the Australian public a stable security industry composed of persons, firms and corporations who are fit and proper to assume the responsibilities and trusts required of the security industry; and

- to provide information and advisory services and appoint spokesmen, public relations consultants and other experts to advise.

ASIAL is not perfect, but over the years it has gained credibility both in and out of the PSI, and standards are set for its members. ASIAL has also been in the forefront of setting standards and is also a representative of the Standards Association of Australia.

Australian Standards

The most relevant standard covering the security industry is Australian Standard 2201, Parts 1 and 2 (Standards Association of Australia 1986). Part 1 covers intruder alarm systems and Part 2 the central station and signalling links. This part of the specification sets out the requirements for central stations, proprietary stations and other remote stations, and also specifies the requirements for landline signalling links between intruder alarm systems and such stations.

Central stations are classified according to their degree of security. The classes are designated Grade 1, Grade 2 and Grade 3 with Grade 1 being the highest security. A few examples of the requirements for central station construction are:

- Grades 1 and 2 the perimeter walls, floor, ceiling and/or roof shall be of substantial construction and equivalent to:

  a bonded brick 228 mm thick, or
  b reinforced concrete 152 mm thick, or
  c pre-cast concrete slabs 152 mm thick, or
  d a cavity brick wall consisting of two 100 mm thickness of brick separated by a 50 mm cavity.

  The construction shall have a fire rating of not less than one hour.

- Grade 3 shall have the walls of at least single brick construction and, if without a concrete floor and ceiling, have a steel lining of not less than 1.6 mm at both floor and ceiling level.

- All grades of central stations shall be located within the premises so that the interior of the room is not in any way visible from outside the premises.

  The normal entrance door and emergency door shall be of armour plate or similar bullet resistant glass. The normal entrance shall consist of two doors forming an airlock not exceeding $4m^2$ and these shall be solenoid operated door releases.

- One of the main features of the Grade 1 central station is all of its equipment is of the dual redundancy type. The specification continues in much the same manner covering: air conditioning, power supplies, emergency lighting, fire protection, air breathing respirators, telephones, direct connection to the police station, two-way radio communication, standby radio equipment, speech facilities, and signalling to the relevant standard.

These standards only broadly cover some of the requirements placed upon the company wishing to supply monitoring services. To obtain a grading, a company must undergo rigorous inspections by various semi-government departments prior to ASIAL issuing a compliance certificate. This procedure is then repeated annually for the company to maintain a current licence.

The one problem with these Australian Standards is that it is not mandatory for any company to conform, and so the users refer to associations such as ASIAL to ensure they are protected and that services and equipment are at a set standard. Another thing that must be kept in mind is that the Australian Standards set only a minimum standard and not a maximum standard.

Problems Confronting the Security Industry

The first problem confronting the PSI is the rapid growth rate of the industry which is forging ahead and not taking, nor having, the time to consolidate the advances produced to date. This explosion has given the government a great many headaches, and one understandable reaction is for the government to regulate the PSI. This is happening in every state to varying degrees with each state body recreating the wheel. Some of the areas that have come into contact with control by regulation are:

- guards and mobile patrols;
- gun laws;
- equipment standards;
- installation standards; and
- technician qualifications.

There are some areas that need regulation to protect all concerned, and this is the case with handguns, if carried by static guards or mobile patrols. Handguns are used for the same purpose in every state; however, the laws controlling them vary, with no good reason, from state to state. If a major Act common throughout Australia cannot be agreed upon, one can imagine the problems that the PSI faces when it tries to set standards for training its various work-skill classifications.

Perhaps the solution may be that the government protect the general public and set the regulations for firearms, but the setting of standards, training and enforcement be left to the PSI. The general public are protected through civil actions, Departments of Consumer Affairs and the Ombudsman. Let the community set the levels, then the companies failing to supply adequate goods and services will not last long.

The second problem is the increasing inability of both the PSI and the general business community to protect themselves. The laws covering privacy, credit and spent convictions seem to be only to protect the criminals, leaving the community wide open to crime. When any matter has been brought into the public arena then it is public information and the community should have access to that information, if they can show just cause. Access should be quick, accurate and attract an application fee.

Thirdly, there are hundreds of organisations which collect information on criminal or suspected criminal activity. If this information were to be pooled and controlled, a lot of the money that crime consumes could be kept in the general community.

A Typical System and Procedure as Employed by Davids Holdings Pty Ltd

Selection of alarm type

One of the most important selections one needs to make is the selection of the method of communication between the premises being monitored and the monitoring company. There are two considerations here: the high value of stock and its ease of dispensability, and the physical protection offered by the building.

This would suit a Direct Line or Securitel with a dialler used, as an alias function providing the additional information the Securitel cannot cover. Both these systems offer line integrity, but there is a great difference in costs. The Direct Line is preferable; however, the cost of a dedicated pair of copper wires running to the nearest concentrator site could cost thousands of dollars per year. Therefore, if Securitel is available in that area that would be the advisable choice.

Detection devices

Any alarm system installed must be able to cope with little feathered friends, rodents, cats and spiders. So it was elected to protect the perimeter with reed switches on doors and windows and have Dual Tec Detectors as backup which look at entry exit paths and directly at expensive stock. Long passage ways are protected by photo electric beams set up in a dual configuration.

Sectors

To give the best protection and early warning, detectors are connected to the panel so that perimeter alarms and internal alarms can be distinguished at the control room end. Also the detectors covering the high value stock and pathways must be determinable. It is always best to have only one detector per sector as this will allow the monitoring company the ability to pass on to the keyholder better information as to the nature of the alarm.

Monitoring

Monitoring means different things to different companies. For example, monitoring of an alarm system can be obtained for as little as $1 per week. However: *you only get what you pay for*. If one is serious about private security then the selection of the monitoring company would be limited to the companies that show some accountability and comply to the relevant Australian Standards. So Davids Holdings Pty Ltd contacted members of ASIAL and obtained quotes before selecting a monitoring company.

Alarm activation

When an alarm activation has occurred, then the panel on that site must store that information for the benefit of the attending keyholder and be a manual reset type.

Response

With the monitoring company receiving an alarm, a single activation, they are to dispatch a mobile patrolman to secure the site and remain until a keyholder attends. If the monitoring company receives a perimeter alarm followed by an internal alarm, then the activation would tend to indicate that there is an intruder on site and police are to be notified. The next step is to notify the keyholder and have him attend giving him all the details. If no keyholders are contactable after twenty minutes, the response company places an armed guard on site who remains there until the arrival of the keyholder, or he is released. At no stage after a multi-activation is a keyholder to go onto a site by himself.

Security breaches

All security breaches are to be reported and recorded.

References

Delbridge, A., Bernard, J.R.L., Blair, D., Peters, P. & Butler, S. 1991, *The Macquarie Dictionary*, The Macquarie Library Pty Ltd, Macquarie University, NSW.

Standards Association of Australia 1986, *Intruder Alarm Systems: systems installed in a client's premises*, Australian Standard 2201 Parts 1 & 2, Standards Association of Australia, North Sydney, NSW.

THE USE OF INFORMATION TECHNOLOGY STANDARDS TO SECURE TELECOMMUNICATION NETWORKS

John Snare*
Manager
Telematic and Security Systems Section
Telecom Australia Research Laboratories
Victoria

TELECOMMUNICATIONS NETWORKS ARE BECOMING MORE COMPLEX. Traditional voice networks are now being augmented by a variety of data, integrated services and broadband networks. Not only are the networks becoming more complex, but the services they offer are increasingly sophisticated and valuable. Mobile services, international direct dialling, intelligent network services, virtual private networks and, in future, multi-media information services and entertainment services represent an environment where a proactive and consistent approach to security is required.

Security requirements in this context have two perspectives. On one hand, telecommunications networks must be secure against unauthorised actions that could have impacts on the business of the network operator. Thus the network must be available to paying customers to the maximum possible extent, and billing information must be safe. On the other hand, customers expect that information they entrust to networks will be securely handled. The security design of telecommunication infrastructure must take both these perspectives into account. Thus, from a customer perspective the correct services must be supplied, billing information must be correct, and the chances of unauthorised action should be

* The permission of the Executive General Manager, Research, of Telecom Australia to publish this paper is hereby acknowledged.

minimised; for example, action that might affect charging or compromise communicated information. From both perspectives, unauthorised actions should be detected and traceable.

Satisfaction of these requirements will involve a combination of technology, policy, and procedural based solutions.

Communication Service Security Requirements

The security requirements of telecommunications systems can be considered in terms of the data, functions, hardware, software, terminal and network elements that make up such systems. The protection necessary will be provided by combinations of physical, logical, procedural and personnel security mechanisms as appropriate to the circumstances and the vulnerability. Emphasis in this paper is on logical security because it is in this area that many developments in information technology are simultaneously generating a wide range of new threats and a range of new mechanisms for protection. Important logical security services are:

- authentication: corroboration of claims concerning the identity of a remote entity in a telecommunication system;
- access control: protection against unauthorised use of telecommunication system resources (information, processing, peripherals, functionality);
- confidentiality: protection from unauthorised disclosure of information or traffic flows;
- data integrity: proof that data has not been created, altered, or destroyed in an unauthorised manner; and
- non-repudiation: protection against one or both parties involved in communication later denying such involvement (for example, creation or receipt of information, or use of functionality).

Note that these services are not independent (for example, access control requires use of an authentication service) and can be provided by a number of security mechanisms. These security services must be associated with management functions. Such functions:

- set parameters for use;
- control invocation;
- monitor performance;

- log anomalous events and errors; and
- allow audit and tracing where required.

When considering telecommunication service security requirements, it is apparent that some security services (for example, confidentiality) are best applied on an end-to-end basis between terminal equipment. There are others where both networks and end systems need to be involved. For example, it may be important for terminal systems to authenticate themselves on an end-to-end basis in an application such as Electronic Data Interchange (EDI). However, it is additionally important that terminal and network systems authenticate each other to ensure that charging is correct. Furthermore, although essentially transparent to users, there may be cases where different network sub-systems may need to authenticate each other to allow secure service to be delivered. It can thus be seen that delivery of complex telecommunication services—such as enhanced 'intelligent' voice services, value added information services, or customer network management services—requires logical security to be considered carefully in the context of sophisticated security architectures.

The traditional approach to providing security services in a telecommunication network has been to place heavy emphasis on the use of access control mechanisms. Thus confidentiality, for example, was provided by implementation of systems such that unauthorised parties could not gain access to the communication channel.

Considering modern telecommunication networks as simply special purpose computer networks, with increasing customer accessible functionality, leads to the conclusion that higher levels of security protection are now necessary for critical network control and management systems. Similarly, higher levels of security are required for critical customer applications. Mechanisms based on applied cryptography have been developed over the last decade to provide security services of higher quality. Such mechanisms include:

- encipherment (relevant to confidentiality services and other mechanisms);
- digital signatures (relevant to authentication and non-repudiation services);
- access control mechanisms;
- data integrity mechanisms;
- authentication exchange mechanisms;
- traffic padding mechanisms;

- routing control mechanisms; and
- notarisation mechanisms.

Many of the major computer system vendors have now developed sophisticated security architectures for networks of their computers. Telecommunication network operating companies typically implement network architectures that involve a variety of equipment from many suppliers. The designers of such networks need to adopt a design methodology that includes security provision based on a general security policy.

Security policy should include a process that allows specific system characteristics and a relevant risk analysis to produce implementation architectures and implementation plans that are consistent with those of related systems. A proprietary approach to security implementation in this environment is unlikely to be appropriate, but the availability and use of relevant logical security service and mechanism standards has the potential to allow design and implementation costs to be minimised.

Standards as a Basis of a Security Designers Tool-Kit

Within the international standards community, there is a large amount of work being done of relevance to telecommunications and information technology logical security. Broad models and architectures for communicating computer system security are being standardised by the International Organization for Standardisation (ISO) (within JTC 1/SC 21) and the International Telephony and Telegraphy Consultative Committee (CCITT) (within Study Group VII) in the context of Open Systems Interconnection (OSI) (ISO–84, ISO–88). These same groups are also working on the development of protocols to allow secure services to be realised at both network dependent and application specific levels.

Another Group in ISO (JTC 1/SC 27) is developing standards for general techniques for data security, with emphasis on logical security. As a result of such standardisation activity, it is hoped to build up a security implementor's 'tool-kit'. Standardised mechanisms could then be used, in conjunction with security policy and risk analysis, to provide cost-efficient security functions.

The approach being adopted by SC 27 in its standardisation work is to identify requirements that are common to many applications and then develop standards that allow security technology to be re-used in a variety of applications. General usage frameworks are being developed for such common requirements, along with general models for the use of the respective security services. Finally, mechanisms—both protocols and algorithms—are being developed to allow security services to be realised. With a view to ensuring the widest possible applicability of these mechanism standards, mechanisms are defined wherever possible to allow the security level to be selectable. In practice, this means that security-related parameters (such as key lengths) are selectable to allow performance and cost to be traded-off against security level.

Authentication

Although the concept of authentication is apparently quite straightforward, in communications systems there are a number of issues that require careful consideration. The first issue that must be addressed is that of certification of identity. It is important to be able to transfer reliably information through a network concerning claimed identity, and to have confidence that this information cannot be tampered with, replayed, or delayed. However it is also important to have a mechanism in place to link authentication credentials with an actual physical or legal entity to answer questions such as: 'Who says I am who I say I am?'.

This is especially important in cases where communication is essentially ad-hoc rather than preplanned. The approach most developed in the standards arena (for example, CCITT–88) is to use mechanisms based on public key cryptography (asymmetric cryptosystems) and trusted third parties in the process of creating authentication credentials. Such trusted parties do not need to be directly involved in subsequent instances of authentication, but may become involved again in dispute resolution. The mechanisms currently under study for standardisation are based on both public key algorithms such as RSA (RIV–78) and on the newer 'zero knowledge' protocols (FIAT–86).

Alternative approaches are also possible for applications where public key cryptography is not appropriate and where symmetric algorithms such as DES (NBS–77) must be used. In these cases on-line notarisation or key management services provided by trusted third parties are also being standardised (for example, ANSI–85). Such systems are both operationally and technically less elegant and more complex than the public key approach, but have a role in cases where security management must be tightly controlled.

The standards under development generally assume the availability of a cryptographic algorithm of the appropriate type and then specify a usage framework along with protocols for the authentication on either or both parties. Such protocols have a number of variants to cope with different application requirements; for example, different protocols may be appropriate depending on whether an application is store and forward or interactive. In 1991, emerging authentication standards offer system designers choices concerning the use of random numbers, time-stamps, or both, in authentication protocols.

Integrity

Logical information integrity can be assured through the use of either symmetric or asymmetric cryptosystems. Symmetric schemes involve either the use of Message Authentication Codes (MAC) (SA–85), or encrypted Manipulation Detection Codes (MDC). Both these approaches can protect against tampering by third parties, but on their own offer no protection against receiver tampering. Such protection can be provided by including a trusted third party notary in the communication, but this approach is currently receiving little attention in the standards arena.

Approaches to integrity based on public key cryptosystems are receiving considerable standardisation attention currently. Approaches based on 'digital signatures' are attractive because they:

- simultaneously provide integrity protection against both third party and receiver attack;

- provide origin authentication;
- form the basis of non-repudiation services; and
- do not require on-line participation of third parties.

Because public key cryptosystems are relatively inefficient, special approaches must be adopted to handle the protection of large amounts of information. The approach being adopted for integrity standards is to develop a 'collision resistant' compression or hash function to produce an unpredictable message summary and then encrypt that. Development of cryptographically secure unkeyed hash functions for a standard is an unexpectedly difficult task. Efforts are in hand to develop hash functions based on symmetric crypto-algorithms, simple finite field arithmetic, and operations typically used in common public key crypto-systems. Standards are also under development for integrity protocols based on both public key cryptography and zero-knowledge techniques.

Protection of the integrity of short data blocks also requires special consideration, and a standard based on public key techniques has recently been approved for publication as a standard to cover this case (ISO–91.2).

Non-Repudiation

Non-repudiation in a telecommunications environment can take a variety of forms. For example it may be necessary to prove information transfer from originator to network, from originator to receiver, or from network to receiver. It may also be a requirement to have a non-repudiation based on blind receipt. From a network management perspective, non-repudiation services are relevant to tracing authorisation for control initiatives that may have major impacts on the performance of network systems or on the nature of services provided to customers. Within the standardisation arena, work has recently commenced concerning definition of a general non-repudiation framework along with protocol mechanisms based on the use of symmetric algorithms. It is expected that a parallel project will soon commence concerning protocols for use with asymmetric crypto-systems.

Confidentiality

Both symmetric and asymmetric encryption algorithms are essential components for providing confidentiality and other security services. Unfortunately, the USA has vetoed the development of standards for such algorithms within the ISO data security techniques committees, so this element of the security 'tool-kit' cannot be satisfactorily provided at this stage. However, certain important and related matters are covered by prospective standards. Most significantly, an international register of cryptographic algorithms is being established according to standardised procedures (ISO–90). This register will provide an identifier for algorithms that will allow their recognition in security protocols. It also includes provision to record a lot of detail about the algorithms, such as its properties, intended uses and availability.

Standards have also been produced concerning the modes of use of encryption algorithms for providing confidentiality. Such modes cover encryption on a block by block basis, as well as how data can be encrypted as a chained set of characters or blocks (ISO–91.1).

Security Management — Key Management

Key management is an important part of security management, and important in the provision of logical security services. It is hoped that overview standards can be developed that will provide the basis of sound design of critical key management systems. Such work is currently at an early stage, but a key lifecycle approach is being developed that covers consistent requirements for:

- creation;
- certification;
- distribution;
- backup;
- revocation;
- cancellation;
- destruction;
- audit; and
- use in archives.

Evaluation Criteria

Design and implementation of logically secure networked systems presents interesting questions from a security 'strength' perspective. Specifically:

- How does one meaningfully describe the security strength required?; and
- How does one measure the security strength realised in implemented systems?

In the past, these questions have been addressed by the major western countries for military and government systems through various trusted system evaluation criteria and interpretations. A standardised approach is now considered desirable to cover commercial systems and recognise the international nature of procurement.

The conventional approach is also considered to be inadequate in that evaluations are expensive, configuration specific, and biased towards confidentiality. The process of use of government criteria is essentially adversarial in that systems are procured to a security specification, and then an evaluator is hired (with a vested interest in finding fault) to determine whether the supplied goods meet specification. In commercial applications, more of a cooperative approach is seen as desirable. In this case, equipment suppliers can make sustainable claims when products are offered, and after-the-event evaluation avoided as much as possible. Commercial evaluation criteria would also need increased emphasis on security services beyond confidentiality, be flexible in allowing preventative requirements to be traded-off against detection mechanisms, and take into account commercial disaster recovery practice.

Summary of Progress to Date

A security developers standards 'tool-kit' currently contains standards or drafts covering:

- modes of operation of 64–bit and n–bit block ciphers;
- procedures for the registration of confidentiality algorithms;
- a general authentication model;
- authentication based on public key techniques;
- zero-knowledge techniques;
- digital signature giving message recovery (for small data blocks);
- hash functions;
- non-repudiation using symmetric algorithms;
- key management; and
- evaluation criteria for information technology systems.

As this work continues, it is expected that new items will be added to this list.

Conclusion

This paper has taken a look at prevention of unauthorised network activity from a proactive perspective and identified factors that could require future approaches to be more comprehensive than those of the past. Emphasis has been on how emerging information technology standards may be used to make the provision of logical security systems as simple and efficient as possible. Consideration of the emerging risk environment leads to the conclusion that cryptographic techniques will find an increasing role in the provision of satisfactory security levels in both network infrastructure and application protection. Furthermore, security management will be of primary importance to the successful and cost-efficient solutions to network security problems.

Effective and efficient utilisation of the technological developments outlined in this paper will require development of network security policies and security processes that allow requirements to be placed in a consistent business perspective.

References

Fiat, A. & Shamir, A. 1986, 'How to Prove Yourself: Practical Solutions to Identification and Signature Problems' in *Advances in Cryptology: Crypto 86 proceedings*, ed. A.M. Odlyzko, Springer-Verlag, Berlin.

International Standard ISO–10116 1991, 'Modes of Operation of an n-bit Block Cipher Algorithm', International Organization for Standardization.

International Standard ISO–7498 1988, 'Security Architecture', Addendum 2, International Organization for Standardization.

International Standard ISO–9979 1990, 'Procedures for the Registration of Cryptographic Algorithms', International Organization for Standardization.

International Standard ISO-9796 1991, 'Digital Signature Scheme giving Message Recovery', International Organization for Standardization.

International Telephony and Telegraphy Consultative Committee 1988, Recommendation X.509 1988, 'The Directory—Authentication Framework', International Telephony and Telegraphy Consultative Committee (CCITT).

Rivest, R.L., Shamir, A. & Adleman, L. 1978, 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', *Communications of the ACM*, vol. 21, pp. 120–26.

Standards Association of Australia. Committee IT/5, Electronic Funds Transfer 1985, *Electronic Funds Transfer Requirements for Interfaces: Message Authentication*, Australian Standard AS–2805, Part 4–1985, Standards Association of Australia, North Sydney.

Standards Association of Australia. Committee on Information Processing Systems 1985, *Information Processing Systems: Open Systems Interconnection—Basic*

Reference Model, International Standard ISO–7498 1984, Standards Association of Australia, North Sydney.

United States. National Bureau of Standards 1977, *Data Encryption Standard*, Federal Information Processing Standard Publication 46, U.S. Department of Commerce, National Bureau of Standards, Washington DC, The Bureau, Springfield, Va.

United States. National Bureau of Standards 1985, 'Financial Institution Key Management (Wholesale)', National Standard X.9.17 1985, National Bureau of Standards, Springfield, Va.

CLOSING ADDRESS

Des Berwick
Executive Officer
National Police Research Unit
Adelaide
South Australia

THE FORMAL PROCEEDINGS OF THIS CONFERENCE HAVE NOW COME TO AN end and, on behalf of the Australian Institute of Criminology and the National Police Research Unit, I would like to thank all conference delegates for participating in this, the inaugural Asia Pacific Police Technology Conference.

Conference delegates have been fortunate in being able to share the experiences of a wide range of people involved in technology issues as they relate to law enforcement. To those who have spoken at the conference, our particular thanks is extended for the effort that you have put into preparing and delivering papers. Thanks also goes to those individuals who agreed, at somewhat short notice, to chair particular sessions. We appreciate the time taken from busy schedules to contribute to making this, the inaugural Asia Pacific Police Technology Conference, a fruitful and successful venture.

I would like to comment briefly on a few of the themes that have emerged from papers presented at this conference.

Information technology has, naturally, occupied a large number of sessions at this conference. In considering one of the most notable achievements in Australian law enforcement in the last ten years—namely the establishment of various national common police services, the successes of the National Exchange of Police Information and the Australian Bureau of Criminal Intelligence in establishing national systems employed by all jurisdictions—the cooperative spirit now evident within the Australian law enforcement community provides a positive framework for these and other agencies to expand their services into the future. Similarly, the coordinated information exchange facilities addressed by Peter Roberts and Peter Anderson serve to illustrate how quickly and responsibly Australian governments and their agencies are embracing and exploiting information technology.

From another angle, conference delegates were advised of the initiatives of serving police officers in employing computers to aid in police investigations. The development of computerised facial identification systems in two jurisdictions and the attention given to providing detectives with sufficient skills to effectively investigate crimes involving computers gives further evidence to the capacity of law enforcement agencies to identify and pursue their own technology needs.

Of course, I would be wrong to suggest that law enforcement agencies have some solitary claim to successes and advances in information and other technology areas. Law enforcement agencies have been provided with valuable insights into a number of areas where the private sector and academic community have contributed significantly to the application of technology to law enforcement. The latest generation of red light and speed cameras will possibly make us all consider a cruise control on our next motor vehicle! Equally, the contribution by NEC to the National Automated Fingerprint Identification System (NAFIS) administered by the National Exchange of Police Information (NEPI), has assisted in NAFIS becoming, arguably, the world's best national fingerprint system.

The future directions of forensic science, together with advice from experts in a variety of forensic fields, further illustrates our reliance on, and professional management of, technology. The communications area is one of particular buoyancy and change at this time. Greg Ellis, Alan Rutherford, Ralph Saunders, Neil Preston, John Snare and Bruce Window have all contributed greatly to our appreciation of this complex and exciting field. These are but a few of the issues that have emerged from this conference. With further reflection, I am sure conference delegates will be able to identify many more.

In his opening address, the Federal Minister for Justice, Senator Tate, noted that Australian law enforcement agencies had made a considerable investment in the application of technology to assist their work. He further noted that, to succeed in combating crime, law enforcement agencies must be smarter than the criminals. I submit that during this conference we have received substantial evidence of just how smart Australian law enforcement has become. This is, of course, no reason to become complacent, either in the adoption of technology, or the manner in which it is employed.

On a final note, one issue kept emerging in a number of sessions. That issue was the absolute need for the use of technology to achieve law enforcement agencies' functional requirements. To quote from Barry Jones' seventh law in his book, *Sleepers Wake!: technology and the future of work*:

> Every technological change has an equal capacity for the enhancement and degradation of life, depending on how it is used (Jones 1982, p. 257).

Law enforcement agencies must always be sure that the technology employed is there to serve them. All too often in the past, it has been law enforcement officers who became the servants, and technology the master.

In closing, I hope that all delegates have found this conference to be stimulating and productive. The variety and number of formal sessions presented, combined with the opportunities for informal discussions with contemporaries from law enforcement, academic and private sector agencies has, I am sure, provided something for everyone. I would particularly like to pay tribute to the staff of the Australian Institute of Criminology and the various National Police Research Unit staff involved in planning and staging the conference. Thank you once again. The 1991 Asia Pacific Police Technology Conference is now declared closed.

Reference

Jones, B. 1982, *Sleepers Wake!: technology and the future of work*, Oxford University Press, Melbourne.