CRIMINAL JUSTICE
COMMISSION

SELLING YOUR SECRETS

PROCEEDINGS OF A CONFERENCE ON THE UNLAWFUL RELEASE OF GOVERNMENT INFORMATION

SEPTEMBER 1993

ISBN 0-7242-5708-X

Criminal Justice Commission
557 Coronation Drive
Toowong, Queensland

Postal Address: PO Box 137
Albert Street
Brisbane 4002

Telephone: (07) 360 6060
Facsimile: (07) 360 6333

ACKNOWLEDGMENTS

The Criminal Justice Commission and The Royal Institute of Public Administration Australia (Queensland Branch) would like to take this opportunity to acknowledge the contributions of:

Mr Ian Temby QC, Commissioner, Independent Commission Against Corruption

Mr Barry Smith, Director-General, Department of Justice and Attorney-General

The Honourable Mr Justice Spender, Federal Court of Australia

Dr Jim Hann, Manager, Information Technology Planning, Queensland Police Service

Major Nicholas Chantler, Justice Studies, Law Faculty, Queensland University of Technology

Mr Kevin O'Connor QC, Commissioner of Privacy, Human Rights and Equal Opportunity Commission

Mr Graham Jones, Regional Manager, Insurance Council of Australia

Mr Chris Bishop, Director, Legal, Australian Bankers' Association

Mr Tim Dixon, Director, Australian Privacy Foundation

Ms Janine Walker, Director, Industrial Services, State Public Services Federation of Queensland

Professor Chris Gilbert, Clayton Utz Professor of Commercial Law, Co-Director, Centre for Commercial and Property Law, Queensland University of Technology

The Honourable Adrian Roden QC.

The organisers of the Conference also wish to acknowledge the assistance of Qantas Airways in the sponsorship of this event.

TABLE OF CONTENTS

SESSION 1

Federal and State Perspectives

CHAIR: Robin O'Regan QC
Chairperson
Criminal Justice Commission

WELCOME ADDRESS

Robin O'Regan QC

Ladies and gentlemen, I am very pleased to welcome you to this seminar on the Unlawful Release of Government Information, which is presented jointly by the Criminal Justice Commission and the Queensland Branch of the Royal Institute of Public Administration Australia.

One of the responsibilities of the Commission is to stimulate community debate about the detection and prevention of official misconduct, and one fashionable form of official misconduct at present seems to be the illicit traffic in Government-held information.

In 1992 the Independent Commission Against Corruption published a report which disclosed an extensive illicit trade in such information in New South Wales. The report was the result of a most extensive investigation lasting many months and involving the testimony of numerous witnesses.

It revealed that the principal participants in this trade were public officials who had corruptly sold confidential information entrusted to their care; private inquiry and commercial agents who acted as brokers and retailers and provided the link between the buyers and the sellers; and the buyers who were the financial institutions and other enterprises who provided a ready market for the information.

The Honourable Adrian Roden QC, the author of the ICAC report, said in February this year that there was no reason to believe that this trade had disappeared after his inquiry.

Furthermore, the keynote speaker today, the Commissioner for the ICAC Mr Ian Temby QC, in releasing the papers of the Sydney conference on this subject earlier this year, said:

> There is absolutely no reason to imagine that the problems revealed by the Commission's Report are limited to the State of New South Wales. Indeed there is every reason to imagine that the position here is more or less replicated in other parts of Australia and indeed in similar societies overseas.

I am grateful that he has agreed to address this seminar and to indicate for us the nature and extent of the problems revealed by ICAC's investigations.

This seminar will be presented in four sessions. I will chair the first session, which will consider Federal and State perspectives. The second session will be chaired by CJC Commissioner John Kelly, and that will discuss the issues involved in computer-based information theft.

After lunch, the third session will be chaired by CJC Commissioner Lewis Wyvill QC, and representatives from large private enterprise organisations will then have an opportunity to give their views. It is important that this be done because the ICAC report named financial institutions as the principal buyers of this illicitly acquired information.

The final session will be chaired by CJC Commissioner Barrie Ffrench, and will provide an opportunity for a union and community response.

In the first session, the keynote address will be given by Mr Temby QC. Other papers will be presented by Mr Justice Spender of the Federal Court of Australia and Barry Smith, the Director-General of the Department of Justice and Attorney-General.

In introducing this first session, I observe that the investigation which has prompted the CJC to present this seminar was carried out by ICAC which, like the CJC, is not a privacy commission but an anti-corruption organisation.

Mr Kevin O'Connor, the Privacy Commissioner, in a paper to be delivered in the second session, may discuss the conflict between maintaining privacy of personal information held by government agencies, and the claim made by commercial agencies to the right to access to some information for commercial purposes. This, of course, is a matter of great importance but is not the major issue in this seminar.

The Commission's clear objective today is to place the corrupt practices involved in the unlawful release of information on the public agenda.

ICAC has done a considerable public service by demonstrating that private information relating to Australian citizens has become a marketable commodity in a traffic between private investigators, banks, finance companies, police and public servants and that there now exists an extensive, costly, and corrupt trade.

I now invite the Commissioner of the ICAC, Mr Temby QC, to address you.

KEYNOTE ADDRESS

Selling your secrets: The ICAC Investigation Into the Release of Government Information by Ian Temby QC

In May 1990, a team of NSW police officers executed a search warrant on the premises of a private investigator name Stephen James. They found there a substantial quantity of official information on individuals, including criminal history and driving licence particulars. A grave problem was thus uncovered. Police or other public officials had given out information meant to be confidential. The police rightly thought a criminal investigation and prosecutions might not solve the problem. Accordingly they sought assistance from the Independent Commission Against Corruption (ICAC). Then commenced what became a very large investigation, which led to a report in August 1992. It contained many recommendations and 273 specific findings of fact. The first four of them demonstrated some of the issues which emerged from the investigation:

1. Over a period from about 1982 to 1989, Stephen James corruptly purchased confidential police information from Senior Constable Terence Watharow, a serving police officer. It included information from RTA records, criminal histories and other police records.

2. Constable Watharow released the information he corruptly sold to Mr James, without authority and in breach of his duty as a police officer.

3. In the course of obtaining that information, Constable Watharow from time to time used the registered numbers and personal access codes of other police officers to gain unauthorised access to the police computer system.

4. Constable Watharow, with authority, also gave Mr James information relating to police methods of storing and releasing criminal records both manually and by computer. Mr James used that information to obtain criminal history information by telephone, falsely representing himself to a police officer when so doing.

What was Watharow selling to James? Personal information about citizens including licence and car registration particulars, addresses and criminal history details. All of it gathered by government. All of it supposedly kept confidential. As other findings made clear, James was selling them to various clients, including financial institutions and solicitors.

Confidential information on individuals was however not the only commodity traded between Watharow and James. As indicated in the fourth finding of fact, Watharow also supplied information to James which allowed him to directly compromise the integrity of records maintained by the police. Using information provided by Watharow, James successfully set about obtaining information from the police database without the necessity of compromising himself by use of a go-between. He even considered "hacking" into the police computer system. That the system was capable of being so compromised with so little apparent effort and with potentially serious implications raised a number of concerns. Once having agreed to supply details of individuals, it is but a small step for a corrupt public official to provide information on how to compromise the system which stores that information. Government therefore needs to be on guard against not only the release of information on individuals, but the release of information which compromises the system that stores that information.

James provides yet another example of how improper access to confidential information can directly affect the integrity of public records.

In June 1986 James knew a New Zealand man, the holder of a New South Wales driver's licence valid until 9 November 1986. The New Zealand man left Australia without renewing the licence. At that time James did not have a driver's licence in his own name, having been disqualified or unlicensed throughout the period from March 1982. As late as October 1986 he had been convicted of a driving related offence and disqualified from driving for a period of three years.

In March 1987 he presented himself at an office of the Roads and Traffic Authority falsely pretending that he was the New Zealand man, and seeking to renew the licence which had lapsed almost four months earlier. In order to do that it was necessary for him to ensure that the New Zealand man had not renewed the licence and to be able to prove his identity. Accordingly he had Constable Watharow check the licence details. It was a relatively easy matter to arrange evidence confirming his "identity" as the New Zealand man. The licence was ultimately renewed on 17 March 1987 with a new expiry date of 9 November 1987. From time to time James notified changes of address on the licence. He continued obtaining renewals of the licence until he finally allowed it to lapse in November 1990.

Of course the existence of such a licence in a false name went beyond enabling James to use it if he had wished to do so whilst disqualified. A licence is a crucial form of identity which can be used to, in turn, create other false documents. And that apparently is what James did. Other documents removed from James included a gas company account in the name of the New Zealand man, a note in James' handwriting including some particulars relating to the New Zealand man, and some telephone numbers including those of the New Zealand Consulate General and the

Rockdale office of the Department of Immigration. The note also contained the address of the Taxation Office alongside which was written 'take some ID and obtain the old tax file number.'

Although there was no evidence that James actually did anything more than I have recited with the false identity he had created for himself, this collection of documents and his note provide a telling indication of the use to which improperly obtained government information can be put.

The Commission initially envisaged the investigation would be limited to James' involvement in obtaining confidential information, and to those public officials with whom he dealt. It soon became apparent however that the trade was much more widespread. James nominated a number of officials employed by the Roads and Traffic Authority as persons who have supplied him with confidential information from that source. Those officials eventually admitted their dealings with James and nominated other private inquiry agents to whom they had supplied information. In following up those leads the Commission eventually uncovered a vast multi-million dollar trade in confidential information involving not just public officials and private inquiry agents, but also some of the nation's leading financial institutions. Although James played a role in that trade he was by no means the major player. Many other private inquiry agents had access to an even wider range of information – and used that access to make considerable sums of money from themselves.

In all, the report names 155 persons and organisations as having engaged in corrupt conduct, and a further 101 as having engaged in conduct liable to allow, encourage or cause corrupt conduct. Those listed include some of the nation's leading banks and insurance companies. Of the many public officials found to have improperly released information on citizens they are supposed to protect, 37 were serving police officers at the time. The ranges in rank were Chief Superintendent down to Constable. Eighteen of them were still in the Police Service when their evidence was taken. Another principal source was the Roads and Traffic Authority, 14 of whose serving officers were involved in the improper release of information.

The departments and agencies from which information was improperly released was not just State bodies – Police RTA and County Councils – but also such Commonwealth bodes as the Department of Social Security, Telecom, Medicare, the Department of Immigration and the Australian Taxation Office.

The picture which emerged was that if information was needed, then it was just a matter of having the right contacts and a willingness to pay. Most often the information was sold by public officials. However that was not always the case. In some instances the information was provided on an exchange basis. A number of public officials working for government departments or agencies supplied

information to debt collectors working for finance companies or banks to allow the latter to chase up bad debtors. At times they in turn were provided with information from those institutions in relation to people in whom they had some interest.

An example of how the exchange arrangement sometimes worked is that of Mrs Wilson. She had 20 years experience in the debt recovery industry having worked for a number of finance companies. Mrs Wilson obtained information free of charge from various public officials on an information exchange arrangement, and then sold the information to a firm of private inquiry agents. She reciprocated by releasing to her suppliers confidential information obtained through her employer's membership in the Credit Reference Association of Australia.

By and large it was money that generated the trade. Anything could be and was purchased. That included information from taxation and Department of Social Security records. The public has been assured, time and time again, that these records are secure. They are not. You will remember the Australia Card debate several years ago. The issues raised were nothing new. The trade on our secrets began a long time ago.

Most of those who acted as information brokers were private inquiry agents, and many of them were former police officers. Some had resigned while under investigation, and were unscrupulous by nature. They could obtain address and credit information for the purpose of debt recovery. There is no reason to believe they could not obtain current addresses with a view to enabling recovery of illegal debts, for example, money owing for narcotic drugs. It is a notorious fact that drug dealers sometimes cause their debtors to be killed, in order to send a stern message to other debtors. Information could be purchased about movements into and out of the country, about the medical condition of individuals, about pension entitlements, and so forth. All of it could be used for good or bad ends. It is generally true to say that confidential information held by New South Wales and Commonwealth Governments about citizens could be bought by anybody if both the willingness and the contacts were there.

And the trade was massive. Consider the following examples:

> One private inquiry agent, Kent Rindfleish, literally conducted a multi-million dollar business trading in the secrets of citizens. With his various contacts he was able to supply RTA, local council, social security, electricity and immigration information, post office box numbers, telephone accounts and even silent telephone numbers.
>
> He obtained RTA information from an RTA employee. Payments to that employee alone over the last twelve months of his dealings were estimated by the public official involved to be about $1,500 per month.

Money paid to his social security source, as estimated by Rindfleish, was between $40,000 and $50,000 per year.

That of course was only one half of the equation. Rindfleish on-sold the information he obtained to his clients. Supply of confidential information was not only a mainstay of Rindfleish's business, it also provided him with a large income and allowed him to accumulate great sums of money. In one account alone he had a balance of close to $1,000,000.

Another example is that of Jeffrey Betts, an employee of the RTA. He supplied information from this employer's records to a number of private inquiry agents. He admitted that on his own calculations he had received about $70,000 from this three major clients alone. Taking into account their records and also his lesser clients, that figure grows to in excess of $100,000. Some of the information that he provided to his clients was information that was available from the RTA for payment of a fee. His charges were less than the official rate. He was also able to process inquiries at a faster rate than would have been the case if an official request had been made. His activities, therefore, and those of officers in similar positions, deprived the RTA of a large amount of revenue.

An even more notorious supplier of confidential information was Detective Senior Sergeant Michael O'Connell, who was, at that time, in charge of detectives at a Sydney suburban police station. The Commission's investigation revealed that O'Connell had been accessing confidential information from the police computer system for sale at a rate of in excess of 3,000 checks a year. Apart from using his own access code to obtain information, he also utilised the personal access codes of four other police officers. He also used his positions as a police officer, and a false pretence that he was on police business, to induce an employee of the Department of Social Security to disclose to him confidential social security information which he then sold to private investigators. He also traded in confidential Telecom information, including information about silent telephone numbers.

He eventually admitted dealings with seven private inquiry agents. He said that he could earn as much as $560 for checks done at a single sitting at the police computer terminal. His processing of confidential information was so extensive that one private inquiry agent installed a facsimile machine at O'Connell's home in order to handle the workload.

People such as Betts and O'Connor paid no income tax on their illicit gains.

Many other examples could be given. The point is that the trade was massive, not only as to the types of information that could be provided, and the volume, but also in the amounts of money involved. It was a multi-million dollar trade, which, until the Commission's investigation, had remained hidden from public scrutiny.

Without a market, the trade would not have existed. The market demand for the types of information provided was largely, but not exclusively, generated by organisations seeking information in relation to bad debts. That largely involved banks and other financial institutions, but also from time to time others, including government departments or agencies.

Some of course claimed they were unaware that there was any illegality or impropriety involved in the information they sought. In many cases however that was a difficult proposition to accept, particularly given the extent to which some organisations went to disguise their participation in the trade. For example, the ANZ, National and Westpac banks used a system of codes to disguise the type of information they sought and obtained.

Some organisations even tried to destroy documentation in an attempt to hide their involvement from ICAC officers. Staff at the Advance Bank for example were caught out in a systematic attempt to alter records to disguise the fact that their bank had obtained such information.

Now, ladies and gentlemen, how does all this relate to the good people of Queensland? That leads to an obvious question. Is the problem confined to New South Wales? Is there something about the air in Sydney or perhaps the water, which leads to such practices? I do not believe so.

There is every reason to believe that what the ICAC uncovered is replicated throughout Australia, and indeed throughout the so-called developed world.

The first evidence I offer is that the sales effected were not confined to one government as has already been made clear. This was not a problem unique to New South Wales.

Secondly, shortly after release of the Report, I addressed an international gathering of privacy commissioners in Sydney. This is just the sort of conduct that these people are most especially concerned about. Nobody present had any doubt that the same sort of problems, perhaps in a slightly different shape, and perhaps to a greater or lesser extent, were occurring in their respective countries. They had seen nothing as extensive by way of disclosure in their own jurisdictions, but readily recognised the real reason. It is not that New South Wales has a special problem. The point rather is that we have a body with the powers and capacity to document the problem in all its painful detail. So does Queensland, but most other places lack such mechanisms.

The third point worth mentioning proceeds from the systems deficiencies which the ICAC report disclosed. Those deficiencies are not confined to New South Wales but, to varying degrees, exist at all levels of government throughout the Commonwealth.

At the time of the Commission's inquiry there was no set policy among New South Wales government departments and agencies for the handling of personal information. In some cases what was regarded as confidential by one agency was made freely available by another. Nor was there any settled practice for the instruction or education of staff who handled information or had access to it. Information exchange arrangements and practices in a number of departments and agencies developed through the initiatives of individual officers. In consequence, access to information in many instances depended on unofficial personal contacts rather than official policy. In some cases public officials were unaware of their organisation's policies, or only had an incomplete understanding of those policies and their implications. A lack of education and staff training often contributed to the problem.

Along with the lack of co-ordinated policy, lack of adequate security was a factor in development of the corrupt trade. There are two important aspects of security. One is protection of the information, designed to prevent access by unauthorised persons. The other is registration of accessed material, designed to provide a record of the person responsible for each access. Modern systems of electronic storage of data can be protected by providing authorised persons with specific access codes or passwords. This has been done to a varying extent and with varying degrees of success by some departments and agencies, but by no means all. The use of personal access codes is a useful method to record who has had access to what information at what period. This allows organisations to run audit trails to discover who has accessed information that has been improperly released. It also enables organisations to undertake "spot checks" on those entitled to access. Such "spot checks" can be used to ascertain if a particular officer, or a group of officers, is accessing the computer database more often that is justifiable given their duties.

In some cases such security arrangements already existed. That was particularly the case with the New South Wales Police Service. The value of the system however was greatly diminished by a lack of security consciousness, a general laxity in handling and using codes by police officers, and a lack of care in establishing and maintaining the necessary records. For example, at the time of the inquiry, a number of abuses occurred with use of personal access codes by police officers. Many used their nicknames as their access codes, as was commonly known. Some openly disclosed their codes to others. Many did not change their codes for years, despite the procedures for doing so being straightforward. At times a program, accessed by one officer by use of his own code, was left open for others to use. Codes remained operative at times when their users were on extended leave, or even suspended. And I could go on.

The Commission's investigation established that some officers used the codes of others to access the police computer system and extract information for sale to private investigators. In that way the release of information could not be easily

traced to them. I am happy to say that as a result of the Commission's inquiry, the New South Wales Police Service undertook a review of the security arrangements attached to access to their system, which has resulted in production of a much improved system.

Part and parcel of the systems failures identified by the Commission was a failure by some public officials to comply with required standards of honesty and impartiality. There was also a failure by some public authorities to properly instruct and educate their staff as to ethical use of information collected by those authorities.

Does all of that sound familiar? If you can say that Queensland has

- effective laws against bribery and official insubordination;
- an effective regime for data protection, including audit trails;
- which regime is vigorously enforced; and
- a strong commitment to raising public sector ethics in all departments and agencies

then perhaps you have nothing to worry about.

But I suspect that some of these conditions do not apply in this State. Indeed I suspect that none of them apply fully. If so, you have a problem. I do not doubt that an investigation in this State would uncover similar and equally extensive corrupt conduct.

If that is right, certain consequences necessarily flow. The secrets held by government about its citizens are being sold. Many public officials are corrupt. So are many brokers, private inquiry agents, and many within purchasing institutions such as banks, finance companies and insurers.

What should be done about it? All concerned could accept that what we discovered in New South Wales also prevails here, and proceed to address the problem. That would save a great deal of time and money, to be measured in years and millions of dollars. Otherwise the situation must be investigated and fully documented.

Education, policy formulation and data security are, as set out above, important preventative issues. In the event however that such measures fail to prevent or deter the release of information reliance must be placed upon the law to adequately enforce confidentiality of private records. The investigation highlighted a number of deficiencies in the law which need to be addressed. Inadequacy of current law at both State and Commonwealth levels is demonstrated by an unsuccessful prosecution in 1990, shortly before the Commission's investigation commenced. A

private inquiry agent had for some time been advertising that he could provide a variety of State and Commonwealth government information. The information on offer was shown in various brochures published by him as including RTA, social security, Medicare, Immigration, telephone, post office box and criminal history information. His dealings in social security information led to his prosecution. His brochure described what he referred to as a 'no. 2 check':

> A search of Social Security records. This search will ascertain if a debtor is receiving a pension or unemployment benefits. It will give the latest address on record and the date of last payment. This search can be carried out in all states. $20 for Australia wide searches.

The agent was charged under Commonwealth legislation with being knowingly concerned in an unauthorised communication by an unidentified officer of the Department of Social Security. To succeed in the prosecution it was necessary to establish that an officer of the Department had released the information to him. Ultimately the prosecution failed because it could not be shown, beyond a reasonable doubt, that an officer of the Department had released the information to the defendant. The information could have been obtained by other means, such as through someone who had hacked into the Department's computer system, or by the defendant hacking into it himself. The New South Wales RTA and criminal history information he was advertising and selling was obviously obtained by improper means and without authority. New South Wales police investigated, but the Director of Public Prosecutions decided against further action.

Whilst the sale of information by a public official involves illegality both on the part of the public official and the purchaser of the information, the provision of information by a public official, free of charge, but contrary to his employer's policies, does not necessarily involve a criminal offence. At most it may simply involve a disciplinary offence or grounds for dismissing the public official. The recipient of the information may have committed no crime, even though he was aware of the impropriety involved in seeking and obtaining the information. Even when the information has been purchased from a public official, the ultimate recipients of the information, provided they are not involved in any payment to the public official, may avoid any criminal consequences.

The problem is that possessing and handling confidential government information is not an offence. In New South Wales alone 39 different statutes have been identified which prohibit the unauthorised disclosure of information from different government departments or agencies. Each provision has its own forms of words and its own penalties. There is no general prohibition, in the absence of bribery of a public official and improper access to data stored on a computer, on trading in such information. A major recommendation made by the Commission was that information be classified. Information classified as confidential or restricted should be regarded as a prohibited commodity, like prescribed drugs or stolen goods. It

should be an offence not only for public officials to release such information, but for others to deal in it or disseminate it in any other way, without authority.

Does confidentiality really matter?

There are of course those who say that a way of preventing abuse of the system is to make such information freely available either to the public generally or to specific classes of the public. This is an ingenuous argument. It is akin to saying that the practical way of dealing with abuse is to legalise it. In that way it is no longer abuse. Imagine suggesting that one way to deal with burglaries is to decriminalise them. Imagine the outcry that would provoke. Invasion of personal privacy, by the release of confidential information, is in some way like a burglary. In some cases, however, what is being stolen is even more valuable than property, and less definable. It is one's right to privacy. It is protection of confidential information that is provided to government authorities on the basis that it remains confidential and is only used for the purposes of those bodies. Rights to privacy should not be discounted. Indeed such a right is recognised in the International Covenant on Civil and Political Rights which was adopted by the United Nations General Assembly in 1966, came into force in 1976 and was ratified by Australia in 1980. Article 17 provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy,' and 'everyone has the right to the protection of the law against such interference...'

Right to privacy is not the only consideration. The proper functioning of government departments and agencies, and indeed the smooth running of government itself, often depends upon the integrity and accuracy of records maintained by government. Many of those records rely on the accuracy of information provided by individuals. The overwhelming majority of individuals provide accurate information in the belief that the information will be properly protected and not made publicly available. That position however may change if individuals perceive that such information will not be treated confidentiality, or if the system under which it is stored is open to widespread abuse. The ultimate result may be a loss of integrity and accuracy in government records which may affect the functioning of government agencies.

That is not a fantastic view. An example already exists in relation to electoral rolls. All Australians over the age of 18 are required to register to vote. They must supply their name and address to the Australian Electoral Commission. This information is then printed on to electoral rolls which are publicly available. Voters are required to update that information each time there is a change in their address. One might be forgiven for thinking that all private inquiry agents needed, in order to trace addresses, was access to the electoral rolls. Of course they have access to those rolls, but have found them notoriously unreliable. Indeed in the Commission's experience in trying to locate various private inquiry agents, it was

often the case that they were either not registered or were registered under old or non-existent addresses. The point is an obvious one. People know that the information supply to the Electoral Commission becomes publicly available. Those people who have concerns that their privacy or rights might be affected by disclosures of their address simply do not provide accurate information, even though not to do so is an offence. The result is that the electoral rolls are not reliable records. Imagine what consequences might flow if other records held by government agencies or departments became similarly compromised.

Creating a new liability?

There is a further reason why public authorities should be concerned to maintain confidentiality of information which they obtain. Given the increase in the type and scope of personal information obtained by government departments and the increasing concern by the public about the security of that information, we may well see the development, both in this country and overseas, of new legal doctrines on the ownership of such information which ultimately could result in the development of civil litigation and the award of damages against those public authorities which, through their negligence, improperly release confidential information. A recent English case suggests the beginnings of the development of such a doctrine.

In *Marcel v. Commissioner of Police* (1992) Ch. 225 British police seized a number of documents for a criminal investigation. They subsequently made some of those documents available to a party engaged in civil proceedings against the plaintiff. In considering the issues involved the court held that where a public authority is given powers to obtain information or documents from a private citizen for a limited purposes, that gave rise to a duty of confidentiality not to use the information or document for any wider, unauthorised purpose. The court held that the right to enforce the duty was not absolute but had to be balanced against any other conflicting public interest. That would include the provision of information to law enforcement agencies. While that decision did not go to the extent of suggesting that the aggrieved party might be able to claim damages against the public authority, it is nevertheless a landmark decision and one which, I suggest, is likely to be followed in this country should the occasion arise. It is probable that further development of the principles raised in Marcel may include the recognition of a right by citizens to seek damages from public authorities for the unauthorised release of their confidential records. To avoid such liability public authorities will need to take much more seriously the need for, and implementation of, policies and procedures for the protection of such information.

I speak now by way of conclusion. The Commission's investigation uncovered a multi-million dollar trade in confidential information. Although the investigation was essentially limited to the position in New South Wales, there is no reason to

suspect that the problem does not exist in other States. Indeed, there is every reason to believe that it does so exist.

This trade needs to be combated by the implementation of effective and appropriate policies and educational programs by public authorities. Those programs need to be continuing if they are to be fully effective. They need to be enforced by appropriate penalties for those who release the information and for those who deal in such information. For public authorities, and for the community at large, the issue is not only one of privacy, as important as that is. The corrupting of our public officials and authorities, the loss of public revenue, the loss of integrity of public records, the loss of confidence in government agencies and departments, all combine to demand that the issue of unauthorised release of confidential information be addressed throughout Australia.

Governments are supposed to look after us, or at least leave us alone. At the moment, through crooked officials, they are selling our secrets.

To understand the concerns, the expectations, the advantages and the harm that can evolve from an interchange or sale of information, we must firstly understand the environment in which we live and work and how much most of us are contributing to this sea of information.

The real question of course is not about the sale or disposal of information, but, rather, the impact that such disposal may have on the privacy of the individual.

Although privacy is defined in the *Oxford Dictionary* as 'reserved or belonging to or concerned with the individual', informed public debate no longer recognises such a simplistic definition.

In 1983 the West German Supreme Court ruled that its citizens had the right to 'informational self determination' but most countries have come to a realisation that with the growth of sophisticated technology, there can be no explicit guarantee of personal privacy.

Nor is it fair to attribute any abuses of privacy solely to the super-electronic highways by which personal data is collected. Privacy is invaded not by those devices, but by those who use them. As Marc Rottenburg, a national director of computer professionals in the USA said, 'it is hard to turn off the faucet of technology'.

Indeed, new computer and telecommunication tools are capturing and analysing all kinds of information from a whole range of sources, provided in the first instance for one particular purpose, but which, when linked with another database, can be traded to the highest bidder.

If I were to address the topic for today's discussion in a strict legalistic form – What is the 'government's attitude to the unlawful release of its information' – the answer would be a simplistic one. Under section 4 of the code of conduct for officers of the Queensland public service, no distinction is made between lawful or unlawful release of information. What is prohibited, is the use of official information by officers to gain any kind of advantage for themselves or for another person or organisation. Once it is established that an advantage has been provided, the public servant is exposed to disciplinary action. Under the *Public Service Management and Employment Act*, such disciplinary action may include dismissal. Indeed the code of conduct specifically provides that officers are not prohibited from disclosing official information which would normally be given to any member of the public seeking that information, although there is an embargo upon the information which is of a confidential or private nature from being disclosed without the approval of the chief executive officer.

Despite those provisions, it was recognised in the 1992 report on the review of codes of conduct for public officials prepared by the electoral and administrative review committee that an ethical public sector will not be achieved by simply promulgating a set of principals or rules of conduct for public servants. The Fitzgerald Report had earlier echoed similar sentiments when it stated

> legislative change or changes to the mechanics of public administration cannot of course, be the complete answer to misconduct and inefficiencies. Propriety and ethical behaviour are difficulty to encapsulate in legal and structural terms.

We must also recognise that we have and are continuing to create a community of information seekers. We say that today's kids are smarter, not because of some new gene scientists have developed, but rather because we teach the young to be inquisitive, to be resourceful and to take research to the tenth degree. We humans, like the faucet of technology, of which Marc Rottenburg spoke, also have difficulties in controlling our curiosity, having been deliberately programmed from the earliest days to seek, to find and to use all types of information.

In dealing with either the government or private enterprise, community expectations are now at such a level that client service is usually a principal objective in winning and retaining business. Such service must be fast, accurate and as inexpensive as possible. To meet those service expectations, we all contribute a whole raft of information to a variety of databases, and, although expecting some degree of confidentiality about the information provided, it is usually never a term of the agreement that such information will not be either amalgamated with another database or utilised for reasons other than for which it was provided. One just has to reflect on the information we provide in general banking, buying or selling property, licensing of all descriptions, permits, application for membership of clubs and associations, income tax returns, voting and the myriad of times we use our plastic cards to acquire goods and services. In our modern civilised democracy, we all contribute and recontribute over and over again to the system of information gathering.

Mary Goodenham, writing in the *Globe and Mail* some weeks ago, in an article entitled 'Farewell to the Private Life', said

> every credit card purchase casts a shadow. So does each entry into a security minded workplace or store, application for health insurance, call to a phone sex service, selection of a payer-view movie or movement of a cellular telephone. It is called a data shadow and it grows longer as computer databases record more and more of our daily activities. The image reveals who we are, where we are, whom we know, what we do and when – a sort of electronic alter-ego that is required for us to obtain credit, receive welfare benefits, vote, get a job or cross a border without a hassle. The global village is fast growing into surveillance city.

Governments of all persuasions are often criticised in respect of legislative overkill, where both business and the private citizens accuse the bureaucracy of interfering and hindering business development or restricting individual freedoms and yet there have been pressures particularly in the late 80s and early 90s about the need for further legislative restraint concerning the flow of information which, for some who wish to access data, will be a further inhibitor.

It is often a fine line between the type of information that belongs to an individual and that to which a wider section and sometimes the whole community, is entitled to access. Consequently, privacy may have both a narrow or a wide interpretation depending upon the user and the use to which it is put. Under the catch cry of freedom of the press, privacy is often abused. Take for example the situation where a group of friends meet in a domestic setting to review a closely contested football final. A fight breaks out and one of the parties is subsequently charged with assault. Police, doctors, lawyers, magistrates, court officials are now privy to a number of very personal and private details of the parties and their respective witnesses. Those people of course, have a legitimate right to all that information. However, the court becomes a window to the world and, because the information will sell papers, the press highlight some irrelevant but sordid piece of information, even though during the process of the trial the parties may settle or withdraw from the dispute without recourse to court determination. This information is released to the world in the name of "freedom of the press" without concern for the feelings of the parties, their witness, nor their individual rights to privacy. No one seems to care about the privacy of those individuals about whom information may be stored in the database of several newspapers. Although after specified periods of time the information cannot be republished without penalty it still may be recorded and be accessible. Such intrusion into the intimate lives of some may be catastrophic.

There are those within the community who support the concept that even in the face of moral and community responsibility, certain information about the private activities of an individual should not be accessible. There is another school of thought which suggests that to catch welfare cheats, criminals or corporate wrong-doers, forfeiting privacy is an acceptable practice. They suggest that as a community we have a collective responsibility to stop or to prevent wrongdoers. There are some who take this concept even further and say that as part of community responsibility, all must be subjected to the same intrusions into our privacy for the benefit and good of the community as a whole; for example, the statutory responsibility we all share in relation to breathalyser testing which is undertaken in order to detect drink drivers. I would imagine that to catch a few of those drink drivers, a majority of innocent citizens are inconvenienced, even though slightly, being subjected to questions and testing to determine the presence or absence of alcohol or drugs.

We should also be aware that, when we try to locate the address or assets of a debtor whose very activities may force a business into receivership with serious consequences to the employees of the business, access to that information is often not available. The innocent in those circumstances, are then exposed to public scrutiny, through bankruptcy, or obtaining credit or applying for unemployment benefits and so lose a great deal of their own privacy.

It will be seen from these few examples that we haven't a consistent pattern of thought in the process of what principles of privacy should be applied.

Consider the recent *Four Corners* program on Allan Bond. If we were to take the report at face value, most would say that, to get to the bottom of the saga, all government, all banking institutions, all corporate and personal information should be available for public scrutiny. There would be a strong consensus in the community that privacy principles should not apply in those circumstances to either the corporate or private affairs of Bond and his family. However, if the tables were turned and some organisation was seeking information into our own financial and personal backgrounds which might hurt us, suddenly we would be interested in privacy principles and object to such intrusions. Just to muddy the waters even further, Mary Goodenham to whom I previously referred, says of the Canadian situation, where privacy laws have existed for some considerable time, 'calls for unimpeded access to information are growing louder'.

Consequently, it is a very unstable environment in which the Queensland Government is currently conducting its research into privacy. Are we, as we often do, just destined to follow some other state or Commonwealth legislation into this ever changing environment or should we be seeking an alternative route to protect, as far as is practical, the privacy of our citizens?

What then is the current situation in Queensland? Access to a great deal of information held in government databanks is already available, particularly in circumstances where there is good reason to release it. For example, births, deaths and marriages; vehicle registrations; titles to land; business name searches; are but a few that most people can access without any difficulty, particularly if the information is relevant to the person seeking it.

Much has been said and written about the ICAC hearings concerning the disclosure of confidential government information in NSW and no doubt we will all benefit from those deliberations. That report identified that even the existence of criminal sanctions provided by the *Social Securities Act* did not prevent information from that department being freely traded.

There appears to be three essential matters highlighted in that report as far as government information is concerned.

Firstly, there must be a clear line drawn between information which is available to the public and information which is retained as confidential. The report stated that in the past there had not been any consistent policy to determine what information should or should not be made available to the public. *Secondly*, information that is public should be readily, quickly and cheaply available. In coming to that conclusion, the inquiry found that access to information that indeed was publicly available, had frequently been associated with such delays that a parallel illicit trade had developed with greater speed being its prime selling point. *Thirdly*, information that is to be retained as confidential should be properly protected. That finding, of course, speaks for itself.

In terms of disclosing information held on government databases, there is unquestionably a need to ensure that those responsible for collecting it provide security and unambiguous guidelines for those who work in those environments so that there can be no misunderstanding concerning the availability of the information and on what terms and conditions (if any) it is supplied. More sophisticated systems are already being developed which will, in part, address those needs.

Currently, the transport department is in the throws of setting up a new consolidated database, ironically called TRAILS. This is a new system which will integrate the drivers license register with the vehicle registration system and allow for the efficient exchange of information between jurisdictions. This is justified on the basis of the current trends toward a national licensing scheme.
Trails will have a high level security system by providing full audit trails of access to data. This means that every use, regardless of where the user was, is recorded so that it can be traced back to the user to determine whether the access on any particular occasion was legitimate or unauthorised. We have only to read the fourth Annual Report of the Commonwealth Privacy Commissioner on the operations of the *Privacy Act* to realise that many of the questions and answers to the very vexing issues of privacy have not yet been settled. The report highlights that industry is still grappling with practice and procedures (and at some expense) to protect the privacy of its clients.

The Department of Justice and Attorney-General has recently taken back responsibility for developing proposals dealing with privacy issues and it has been made very clear that the government is serious about privacy considerations. I am reminded of recent negotiations with the Commonwealth about participating in the law enforcement access network system to which the Queensland cabinet gave its "in principle" support, subject to the development of stringent privacy protection initiatives contained either in the memorandum of understanding or by way of specific legislation that set up that system. The Queensland government's concerns were equally shared by the Privacy Commissioner, who wrote about this very topic in his fourth Annual Report.

Some substantial research has already been completed by another department which was formerly investigating privacy issues. It will now be a matter for my department to revisit those undertakings, look at both the local and overseas experience and to place before Cabinet, for its consideration, suggestions which may ultimately lead to the implementation of legislation. This hopefully will not be regarded as over-regulation or as inhibiting access to relevant information. Its purpose will be to benefit the individual and the community by creating a balance between public interest and privacy protection to which we are all entitled.

When counsel for the CJC, Mr Marshall Irwin, asked me to participate in this seminar, I asked myself what useful contribution could I make as a Federal Court judge to a seminar on the unauthorised release of government information.

I have to confess I haven't come up with a satisfactory answer. From time to time I have to deal with claims of statutory immunity from disclosure by the Commonwealth or its agencies. One example was *Lloyds Ships Holdings Pty Ltd v. Defrays Pty Ltd* (1986) 65 ALR 539, which was concerned with the scope of secrecy provisions in the *Australian Trade Commission Act* 1985. The Federal Court, of course, is called upon from time to time to decide similar questions, as well as the extent of exemptions contained in Freedom of Information legislation.

Giving considerable thought to the invitation, I thought that there were three areas in which I might sensibly contribute. The first of those was to outline something of the extent of the legal controls on the provision of government information, both at the federal level and at the state level. This aspect is almost entirely objective.

The second area was to discuss the methods employed by legislation concerning disclosure of government information and to consider the appropriateness of the techniques employed. This area of my contribution is somewhat subjective.

The third area concerns some observations that I make concerning the legal prohibitions that exist against disclosure of government information. This area is entirely subjective.

The legal parameters against disclosure

On inquiry as to the existence of legal controls against disclosure of government information, I was astounded not only by the number of legal prohibitions that exist but also the width of the prohibitions.

In an important article in 1990 in Vol. 19 of the *Federal Law Review* p. 49, entitled 'Secrecy Provisions in Commonwealth Legislation', John McGinness, a Principal Legal Officer with the (Commonwealth) Attorney-General's Department gives an incisive critique of secrecy provisions in Commonwealth legislation.

There are now about 150 separate pieces of Commonwealth Acts and Regulations providing for secrecy in respect of Commonwealth Government information. They range from the *Aboriginal Land Rights (Northern Territory) Act* 1976, *Commonwealth Electoral Act* 1918, *Corporations Act* 1989, the *Crimes Act* 1914, the *Crimes (Taxation Offences) Act* 1980, the *National Crime Authority Act* 1984,

to the *Securities Industry Act* 1980, the *Sex Discrimination Act* 1984, the *Telecommunications Act* 1975, and the *Telecommunications (Interception) Act* 1979.

One can understand secrecy provisions directed at the protection of defence and national security, but the Acts and Regulations set out in the appendix to Mr McGinness's article relate to information over very many areas, which reflect the expansion of the Commonwealth's role since the Second World War in areas such as taxation, health, education, welfare, scientific research, industry research, industry assistance and regulation. The increase in the number of secrecy provisions is also a reflection of the increase in personal and commercially sensitive information collected by the Government, as well as the increase in independent statutory bodies with statutory powers to compel the disclosure of sensitive information, of a business and non-business kind.

The first Commonwealth secrecy provision was in the *Post and Telegraph Act* 1901, which was in fact the twelfth act passed in the first session of the Commonwealth Parliament in 1901. The paramount secrecy provision with respect to Commonwealth Government information is section 70(1) of the *Commonwealth Crimes Act* 1914, which now provides:

> A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he is authorised to publish or communicate it, any fact or document which comes to his knowledge, or into his possession, by virtue of being a Commonwealth officer, and which it is his duty not to disclose, shall be guilty of an offence.

The present penalty is imprisonment for two years. It is interesting that s. 70 originated in s. 86 of the *Queensland Criminal Code* 1889, the first criminal code in Australia.

Also significant is s. 79 of *The Crimes Act*, which is the equivalent of s. 2 of the United Kingdom *Official Secrets Act* 1911. "Prescribed information" is defined in s. 79(1) of the *Crimes Act* to include any information obtained by a Commonwealth officer or person holding office under the Queen which 'by reason of its nature or the circumstances under which it was entrusted to him or it was made or obtained by him or for any other reason, it is his duty to treat it as secrets.' Section 79(3) creates an offence punishable by imprisonment for two years if a person communicates, inter alia, a document or prescribed information to a person other than the person to whom the person is authorised to communicate it or permits a person other than an authorised person to have access to it.

The 'duty to keep secret' requires an officer to keep facts appearing in a document falling within the regulation from public knowledge, or the knowledge of persons other than those nominated in the regulations: *Cortis v. R* (1979) WA Reports 30,

a decision of the Supreme Court of Western Australia. The court rejected the submission that there was a distinction between a duty 'not to disclose' and a 'duty to keep secrets'. It is interesting that the recipient of the information from the State Housing Commission in that case was one *Brian Thomas Burke.*

Of the approximately 150 provisions in Commonwealth Acts and Regulations, more than one-third prohibit the disclosure by an official of any kind of information which he has acquired in the course of his duties. McGinness observed:

> The scope of these provisions reflects a now outdated attitude that, except in very special circumstances, the public has no proper concern with having information about government processes.

Under the *Public Service Regulations* (C'th), there are provisions directed at prohibiting the divulging of official information. Regulation 8A(h) provides:

> An officer shall:
>
> (h) not take, or seek to take, improper advantage, in the interests, pecuniary or otherwise, of the officer, any other person or any group, of any official information acquired, or any document to which he or she has access, as a consequence of his or her employment;

Regulation 37 outlaws the obtaining of benefits to officers as a consequence of taking advantage of that officer's functions.

If a breach by a public servant of these regulations causes harm to a citizen, does the citizen thereby have a right of action against the public servant or the Crown vicariously? Burchett J recently held in *Austin v. Anisette Transport Industries Operations Pty Ltd*, (Federal Court of Australia, unreported, Sydney, 26 August 1993) that the regulations under the *Public Service Act* 1922, which impose duties to the Crown on officers, do not confer upon citizens a private cause of action against the Commonwealth agency.

The Hon Adrian Roden QC, in an extensive report for ICAC, revealed an extensive trade of information in government hands between private investigators, banks, finance companies, police and public servants, amongst others. There is a natural degree of "tut-tutting" about this conduct, particularly when it is done for money. But there are basic questions which still have to be addressed in this area and to which I will shortly come.

I have already referred to s. 70 of the *Crimes Act*. In *Sherlock v. Jacobsen* (1983) 13 ATR 935, Sir Francis Burt, Chief Justice of Western Australia, did not consider a custodial sentence appropriate, in the circumstances of that case, for a

person procuring a breach of s. 70 of the *Crimes Act* by a senior officer in the Taxation Department, the breaches consisting of three instances of obtaining taxation returns of various taxpayers and a fourth charge of obtaining a Queen's Counsel opinion given to the Commonwealth on a tax matter. On the first three charges, a fine of $100 was substituted (the appellant having spent five days in custody) and in respect of the taking from the Taxation Department of the Queen's Counsel's opinion, he was fined $25.

A majority of a Full Court of the Federal Court of Australia, (Bowen C J and Jackson J) held in *Federal Commissioner of Taxation v. Swiss Aluminium Australia Limited* (1986) 66 ALR 159 that the exemption in s. 38 of the *Freedom of Information Act* preventing disclosure if there is in force an enactment that prohibits persons referred to in the enactment from disclosing information of a particular kind, was applicable where the prohibition was that contained in s. 16(2) of the *Income Tax Assessment Act* 1936. That is to say, the effect of the secrecy provision in the *Income Tax Assessment Act* is to substantially limit access under the *Freedom of Information* regime.

I have not attempted a comprehensive survey of Queensland legislation, but it is clear that secrecy provisions under Queensland acts and regulations are similarly numerous and widely expressed.

I have already indicated that s. 86 of the *Criminal Code* is the equivalent of, and indeed was the model for, s. 70 of the *Crimes Act* (C'th). For instance, the *Factories and Shops Act* 1960 s. 10(8) is a blanket prohibition on disclosure to any person any information that a person who is an officer appointed for the purposes of the Act has acquired in the exercise of his functions for the purposes of the Act in a factory or shop. So too s. 10 of the *Stamp Act* 1894-1988; and s. 144 of the *Children's Services Act* 1965-1980 (with some communications to specified persons excepted).

The *Police Service Administration Act* 1990, s. 10.1, dealing with police officers, creates an offence if the information disclosed was not authorised in writing by the Commissioner, the disclosure not being under due process of law, but being information of a confidential or privileged nature which would normally not be available to any member of the public on request. Clause 10.5 imposes liability in the Crown and right of the State of Queensland for a tort committed by any police officer in the course of his employment.

The *Public Service Management and Employment Act* 1985 creates exposure to disciplinary action for wilful failure to comply with any provision of a code of conduct approved by the Governor-in-Council for officers of the public service. Regulation 7 of the *Public Service Management and Employment Regulations* 1988 requires officers to report breaches of s. 29 of the Act. Clause 4.2 of the *Code of*

Conduct in the *Queensland Government Gazette* 1988 p. 7 dealing with the release of official information prohibits the release of information of a confidential or privileged nature except with the approval of the Chief Executive. A new Code of Conduct was recommended in the Electoral & Administrative Reform Commission report on *The Review of Codes of Conduct for Public Officials*. This report was endorsed by the Parliamentary Committee for Electoral and Administrative Reform and is now awaiting consideration by Cabinet.

The legal provisions to which I have referred indicate that there is no doubt that the extensive trade in government information to which Mr Roden in his report referred, constituted unlawful conduct on the part of the officers concerned and those persons who aided counsel or procured the commission of those offences constituted by that conduct.

Part II – Philosophy of the Secrecy Provisions

A very large number of the secrecy provisions are quite general in their prohibition. While the effect of such a prohibition may accord with the general philosophy of the *Privacy Act* 1988, it certainly is in conflict with the underlying notion of freedom of information. The philosophy of such general secrecy provisions seems to be that the public has no proper concern or entitlement to any government information.

There is no doubt that much government information is personally or commercially sensitive. Few would disagree that individual privacy and business secrets are entitled to be respected. Mr Roden QC in his paper 'The ICAC Report and One Year On' said:

> Personal privacy was a casualty of the corrupt trade, as addresses, criminal records, social security particulars, overseas passenger movements and silent telephone numbers all became open secrets.
>
> A considerable amount of argument was heard from commercial interests claiming a right to the information, and privacy watchdogs who urged resistance to the demands for greater access to personal records for commercial purposes.
>
> It is obviously necessary that there be a clear policy with regard to the availability of personal information held by government departments and agencies, either to the public generally or to special interest groups. I took the view that determination of that policy is not a matter for the Commission. What the Commission could properly do, and did, is point to possible corruption implications of the policies that might be considered.

He later said:

> The basic privacy principle involved is that when information is provided under compulsion or in confidence, it should be used only for *the purpose for which it was given, and it should be available only to persons who need it for that purpose. That principle has to yield, however, where it conflicts with a greater public interest, such as the interest in the proper investigation of serious crime. A critical question is what circumstances should be allowed to prevail over that basic privacy principle.*

Is it axiomatic, as Mr Roden QC asserts, that confidentiality has to yield to the investigation of serious crime? If there are qualifications and exceptions to obligations of confidence, is not the public entitled to be cynical, given past history including the wholesale and extensive illegal taping by police officers leading to *The Age* tapes? There do exist grounds for belief that some investigative agencies believe that the end justifies the means, and that the only rule is the eleventh commandment.

The legislative provisions also reflect the desire to protect information suppliers. These provisions are directed not only at the traditional informer but are part of a strategy to convince information suppliers to be more truthful in their disclosures, in reliance on the guarantee of secrecy.

The claimed journalists' privilege from disclosing their sources cannot be absolute, as thoughtful journalists such as Patrick McGinness and Peter Charlton have acknowledged. All circumstances, including the proper administration of justice, must be considered. Perhaps, for similar reasons, there have been successful erosions of privacy considerations for information suppliers in the context of the fight against organised crime and taxation and social security fraud.

However, the marked unpopularity of the Australia Card proposal and the deeply distrustful attitude to the tax file number regime, and the fear of potential misuse entertained by the community generally, is, I suspect, simply a reflection of the fact that Australians do not trust the Government to honour the obligations of confidence which the statutes so nobly proclaim.

It has to be accepted that secrecy provisions can regulate the conduct of public servants; those which permit a disclosure at the direction of a senior public servant or Minister confer a "quarantining power" on the dissemination of information to those persons and therefore underpin their power.

The conflict between the requirements of secrecy and the pull which the exigencies of administration inevitably exerts towards the free exchange of information among fiscal and other government departments, which Dixon J in *Jackson v. McGrath* (1947) 75 CLR 293 at 312 identified as a 'recurring problem' for the

draftsmen, is still very much with us: see ss. 16(4)-16(6) of the *Income Tax Assessment Act* 1936 and the *National Crime Authority (Miscellaneous Amendments) Act* 1985.

In summary, there is, it seems to me, much to be said for the view that the general secrecy provisions to which I have referred should be replaced with provisions applying only to narrow categories of truly sensitive information. If that is done, the aim of privacy protection legislation, which recognises the individual claims to preservation of privacy and confidentiality, can then properly be considered against justifiable claims for the use of information for efficient government. As I have earlier indicated, most secrecy provisions remain as grounds for exemption under s. 38 of the Commonwealth *Freedom of Information Act*, effectively preventing disclosure.

Some observations on the legal provisions concerning secrecy

The first and most obvious observation is the hypocrisy that surrounds them. The public is entitled to be concerned at the illicit trade in government information between private investigators, police officers, banks, financial institutions, public servants and others. The supplying of information for reward seems to be a clear case of official corruption and should be dealt with as such. On the other hand, while governments have strenuously fought in the Courts to maintain the secrecy of cabinet submissions, discussions and decisions in cases where the disclosure might prove embarrassing, it is a notorious fact that the leaking of government information, including even information from Cabinet, is an almost daily occurrence and that journalists are more than willing accomplices in such breaches of existing secrecy provisions.

Governments complain about leaks when it doesn't suit them for that information to leak, yet routinely promote leaks when they perceive it to be in their political interest to do so.

Secondly, the selective application of general laws is inimitable to the rule of law. Where there are repeated breaches of secrecy provisions, but only some are selected for prosecution, the law is brought into disrepute. One example of this arbitrary justice, in a quite different context, appears in *R. v. Zaphir* [1978] Qld R 151 at 180, where Kelly J said of s. 320 of the *Criminal Code* (Qld):

> It is not to be expected that the section would be invoked in circumstances such as those used by way of illustration even though on its strict terms it would seem to apply.

A further and very real matter of concern is the lack of rational distinction between government information which is lawfully available and government information which is not.

By way of example, it is, or was a few years ago, possible to buy a computer disc for about $2500 which contained information concerning the name, address and telephone number covered by all Telecom directories in Australia, so that one could, if one knew a name, find an address and a telephone number, or if one knew a telephone number, find out an address and a name, and so on.

It is not possible in a practical sense to do this just by looking at telephone books, because knowing a number, it would be too time consuming to find out the address or name attaching to that number. However, that information is publicly available. In relation to electoral rolls, it is possible by searching to find out where a person lives provided that person is on the roll. Land holdings and real property securities as well as chattel mortgages and bills of sale, can now be searched in Queensland by computer. Similarly, if a person is involved in a car accident and the police investigate it, one can obtain a police report; in fact, it is a crucial part of the pretrial preparation in cases of personal injury or property damage.

Why should I not be entitled to ask of the police department what criminal convictions a prospective employee might have? There are commercial agencies dealing with credit risk who produce information about persons being sued or judgments that have been given.

Why in that context shouldn't a person considering an application for finance by another be able to ask of a court what judgments have been entered against that applicant? Why shouldn't the conviction of a person be a matter of public record? It occurs in public, it is made in public; similarly a judgment is a public judgment. Why shouldn't these be available?

Finally, I turn to the very heavy duty that lies on bodies like the CJC and ICAC. The CJC is a very well funded body. Its budget is of the order of half as much again the total budgets for the Department of Public Prosecutions and the Legal Aid Office.

Its work is important. It is to be congratulated on holding this seminar. I hope that it will contribute to the emergence of a principled, consistent and coherent regime concerning the divulging of government information.

QUESTION AND ANSWER SESSION

Question 1 — Thank you. Several of the speakers have referred to a number of matters. Mr Ian Temby referred to weaknesses within the system, Mr Barry Smith particularly referred to the electronic age. Part of my concern is what comments would you care to make about what I'd term basically statute weaknesses in the system whereby under some legislation information must be made available to the public. However, the particular legislation had been written in times prior to the electronic age and, consequently, government can now use computer systems to make that particular information more readily available to the public than it would have been when the legislation first came into effect.

Temby — It's not for me to say or indeed suggest what should be done in Queensland. So far as New South Wales is concerned we have recommended that there should be a consistent principal regime of the sort that Justice Spender referred to and much work is presently being done in that respect. One of the major difficulties presently is that there is too much lack of conformity between both statute and practice as between various departments and agencies. So that a given piece of information can be given out by this department but not by that agency. So you've got to have a consistent regime. That's absolutely essential. Where you draw the line is very much a matter of policy which has to be determined by government. It should reflect the will of the people but you can't be dogmatic about that. The proposition that criminal histories which are handed down into public places that is the law represent no more than a collation of public announcements and therefore should be made available on application perhaps for payment of a fee is one that I would not defend to the death. That's a matter for government. It's a matter for the community to decide and for the government to implement. But you have to draw the line and then enforce it. The only other comment I'll make about present statutory weaknesses, at least in New South Wales, and I believe this is true for round Australia, is that if you are dinkum about enforcing data protection you must make it an offence to trade in data which has a confidential tag attached to it. First decide what gets a confidential tag attached, then there must be a law which has to be enforced which makes it an offence to trade in that information. If you only have laws that go back to public officials you can't always nail them. If you want to do something about it you have to get to the private investigation industry not all of

whom are highly scrupulous individuals and deal with those who are trading in such information. That requires the creation of a new offence.

O'Regan Thank you. Any other member of the panel wish to comment on that?

Spender Newspapers and journalists would be very concerned if there were to be an offence created for dealing in confidential information. A journalist can commit an offence if that person counselled or aided or procured the committing of an offence. If, however, the information falls off the back of a truck it seems that there is at least some argument whether a journalist using that information commits an offence. The offence certainly has been committed by someone and there is discussion along the lines of the journalist being akin to a receiver of stolen property in his publishing of that confidential information. But it probably is the case that the journalist in those circumstances doesn't commit an offence as an aider, abetter, counsel or procurer of the breach by the public officer of the duty imposed by the law at the moment. If there is to be an offence of dealing in confidential information, then the journalist probably is called without any questions if the information is truly confidential. In those circumstances there would be singular redundancies in world newspapers.

O'Regan Thank you very much. Barry?

Smith I agree with Ian Temby. Government as a matter of policy has to determine where they will draw the line in terms of what information is to be made public and what information is to remain confidential. I'm quite convinced in fact that if there was some clarity achieved in relation to that matter the corruption which New South Wales found in the public service would be greatly minimised. I believe that over the years there's been no clear definition of what is available from the public record and what should be kept a crime and until we identify those issues then obviously there will continue to be a leaking of information both official and unofficial which may affect the privacy of individuals.

O'Regan Any other questions?

Question 2 In defining privacy and confidentiality would there also be a need to define the release because a government instrumentality or department may make information available just by having it on a

computer system, allowing a hacker to get into it. And there again, you have the media releasing something which was released from someone else which was released from some back of a truck so would there also be the need to clarify in statute the issue of releasing the information? Could you specify in legislation that a department not having adequate controls over computer access is deemed to be releasing information?

Temby — Well it's precisely because you may not be able to establish how information has got out that we have suggested that a new offence of trading in confidential information ought be created. That's precisely the difficulty that I alluded to in the paper. Often you won't know how it got into circulation but having got into circulation we are suggesting it should be treated like stolen goods. Now let me make clear I have no personal difficulty with the proposition that a lot of presently confidential information ought to be declassified. There is a strong tendency for government to pin a confidential label on everything and it's often unnecessary, but it may be a sound proposition that, in relation to the information that we as individuals give government, the rules should be that it can only be used for the purpose for which it has been given. If that rule were applied you'd distinguish between personal information and those enormous amounts of policy information in which the public has significant interest and many assert a right to know.

Spender — The difficulty with the idea that information should be kept for the purpose for which it was supplied runs counter to the exception which I indicated in section 16.4 of the *Income Tax Assessment Act* where for instance a prostitute might make a genuine income tax return and the capacity of that information to get into other hands would be taxed on it and everyone would be happy. There is, however, the real likelihood that that information can be supplied under the rubric of the investigation of serious crime and so you have all these exceptions chipping away at the principle that the information should be used solely for the purpose for which it was supplied. And I don't know quite frankly what the answer is in drawing the boundaries between a person's right to privacy and what is said to be the legitimate concerns of government in relation to the suppression of crime, particularly organised crime and social and taxation fraud, so I simply identified the problem and passed the buck to the mainstream.

Question 3 — Yes I was hoping you would say I don't know what the answer is. I don't find too many people coming up with a solution and I think

that is the thing we really need. I mean Ian Temby was quite right in assuming that it's not only New South Wales – this is the position in every state and every government in the world. So how do you deal with it? Justice Spender made the obvious statement that all information necessary for government should be provided. There should be no embargo whatever in that way. The stupidity is that there's not enough disincentive for those who want to cheat and it's on that basis that I refer the panel to my submissions to the Fitzgerald Report, the *Whistleblowers Protection Act* and Police Powers report in which I suggested some very tough mandatory ways of dealing with these people. I won't say what they are now but I'm prepared to give it to you again. Simply put, it should be not worth it to a public servant to cheat.

O'Regan Do you have any comments, panel?

[no response]

Question 4 My question is directed to Mr Temby. In your opening comments you suggested that in a recent paper that you listed how unlawful release of information in New South Wales continues. After the ICAC Report was released, were you aware of government officials who have been dealt with in accordance with criminal codes etc? I'm also wondering if you could advise us if any private banks, financiers, agents, private investigators etc have at this stage been prosecuted as a deterrent to those people who continue to unlawfully release government information?

Temby I think when the investigation was current we had a strong discouraging effect upon the trade although we did find some people who were called to give evidence on Tuesday were still trading on Thursday and were called back the following Tuesday and had to confess, so some people don't lack gall. But we had a strong discouraging effect which has been of a continuing nature. I would be confident there's been a drop in the trade in New South Wales. I'm not sure about elsewhere. Quite a lot has been done, is being done. A whole series of public officials have been dealt with on a disciplinary basis; many have been sacked, others have been disciplined in various ways. There have been 10 prosecutions commenced, a couple completed, and there are several more coming through the pipeline. There have been no prosecutions of people within the financial community because with the present state of the law they've committed no offences. I have to say that speaking broadly the reaction of the financial institutions has been

somewhat disappointing. They haven't shown a consistent determination to move blameworthy individuals from the areas in which they have had responsibilities to other less sensitive areas, which one would have thought would have been a minimal appropriate reaction. Otherwise, Commission recommendations have been implemented. For example the Police Service has tightened up its data protection control enormously and that's very encouraging indeed, as has the RTA. Other recommendations are still under consideration. There's a couple presently with Cabinet. The position is a quite encouraging one so far as remedial steps are concerned. Mind you you'll never wipe it out. I should say to you that with respect to all the work we do our aim is to minimise corrupt conduct. We do not set out to expunge it because you can't; to do that would be to perfect human nature and that's a very large undertaking.

Question 5 — To some extent the concerns that have been discussed appear to have arisen from an under emphasis by agency managers on properly managing their information resources. There seems to be a disjointed and currently unco-ordinated approach within the agencies. I notice that Public Administration staff at University of Queensland are claiming that they teach information management and I wonder whether the members of the panel might like to comment on whether or not they believe that a co-ordinated approach to the management of government information at both agency and the government level might be likely to contribute to significant improvements.

Smith — Yes.

O'Regan — Very positive Mr Smith.

Spender — I'm always suspicious when someone says I'm from the government – trust me.

Question 6 — The New Zealand government has recently introduced privacy legislation to circumvent any action against personal data and its trading of the European Commission. Is the European Commission privacy legislation likely to impact on Australia and, in that case, is the Commonwealth likely to take over the vehicle?

Temby — I don't know the answer to that question. At the moment we have privacy legislation in various forms at the Commonwealth level and in some states. I would have thought that effective protection

of privacy wherever you chose to draw the line is a challenge best addressed by those who are closely concerned with the problem area. I would have thought that you are more likely to get useful results by forcing action upon the holders of the information by their immediate rulers. Which is to say that to leave the field of the Commonwealth is unlikely to be a step forward. I don't know if it's likely to happen. If it did happen I would think it would be unfortunate.

CHAIR: Well that brings the first session of the conference to a close. I'm sure you all agree with me that it has been a most stimulating and interesting session and has ranged widely over many issues pertaining to this very complex and controversial subject. I should mention that there is another way of describing the phenomena which Mr Justice Spender referred as "things falling off the back of a truck". I heard Mr Beattie being interviewed on television the other night, and he said that, referring to disclosure of confidential information, his colleagues leaked over a very good Chardonnay, which seemed to be an unusual way of describing the thing. But on a more serious note I'm sure you will agree that this has been a session which has established the focus of the debate of this conference very well and the contributions which have been made by individual speakers have been impressive, and I ask you to show your appreciation in the usual way.

SESSION 2

Computer-based Information Theft

CHAIR: John Kelly
Commissioner
Criminal Justice Commission

CHAIR: Ladies and gentlemen: Welcome to the second session of the seminar on the Unlawful Release of Government Information. The general topic is Computer-based Information Theft, and we will also be hearing from the Privacy Commissioner, Mr Kevin O'Connor.

It's a truism to say that we live in a technological age, but we have only recently reached the point when we can say with some conviction that information technology is finally *delivering* all that it has been *promising* for the last two decades. But with this new efficiency in delivery comes the danger that the information also becomes more easily accessible to the wrong people.

Our first two speakers, in their different ways, will address this problem – Dr James Hann is presently on secondment from the Queensland University of Technology to the Queensland Police Service, where he is Manager of Information Planning; and Dr Nick Chantler works in the School of Information Systems at the Queensland University of Technology. I suggest that we hear from both of them and then take fifteen minutes for questions before we change direction a little and hear from Mr Kevin O'Connor, the Privacy Commissioner with the Human Rights and Equal Opportunity Commission, who will address the more general issue of Corrupt Disclosure: the Role of Information Privacy Principles and Practice.

So I now invite first Dr James Hann to address you.

Associate Professor Jim Hann has been with the QPS for three years. His responsibilities include a range of planning and management functions related to the use of information by police. In 1991, following the Fitzgerald Inquiry, he undertook a major review of information services in the QPS, and prepared a comprehensive information strategic plan. Prior to this, he was Dean of the School of Information Technology at the University of Southern Queensland. His research interests are in the fields of information systems planning and organisational performance evaluation, and he has worked as consultant in these areas for several years.

The Use and Management of Information by Police by Dr James Hann

Like many other organisations, the Queensland Police Service has had to review its policies and procedures for the collection, use, and release of information over the last few years. This need has arisen from an increased public interest in privacy issues, privacy legislation, freedom of information legislation, and studies such as the Fitzgerald Enquiry and the NSW ICAC Report on Unauthorised Release of Government Information.

The ICAC Report identified the following causes for the high level of illegal release of government information:

- A lack of consistent policy;
- No settled practice for instructing staff who handle information or who have access to it;
- Information which is normally publicly available is plagued by delays which encourages those seeking it to resort to speedier illegal alternatives; and
- Information which is intended to be kept confidential generally lacks adequate protection measures.

The report stated that if the corrupt trade in official information is to be controlled, three criteria must be set:

- There must be a clear line drawn between information which is publicly available and information which is retained as confidential;
- That which is considered accessible by the public should be readily and cheaply available; and
- That which is to be retained as confidential, should be properly protected.

At present, QPS personnel are governed mainly by the provisions of the *Police Service Administration Act*, the *Freedom of Information Act*, the QPS Code of Conduct, and relevant General Instructions and Commissioner's Circulars.

While the *Police Service Administration Act* creates an offence for personnel to release information in certain circumstances, the purpose of the *Freedom of Information Act* is to extend as far as possible, the legally enforceable right of the community to access information held by the Government. This right of access is

tempered, however, by a recognition in the Act that the disclosure of information in some instances would have a prejudicial effect on essential public interests, or the private or business affairs of members of the community in respect of whom information is collected and held by government.

It is not the function of Service personnel generally (other than those attached to the Freedom of Information Unit) to determine the merits of any application made under the *Freedom of Information Act*. It is, however, the function of general personnel to determine whether a request for information (other than an application made specifically under the Act) can be satisfied at the local level, whether it should be referred to the QPS Information Bureau (an organisational unit responsible for the management of corporate data related to operational policing), or whether it should be referred to the Freedom of Information Unit.

QPS policies and procedures related to the management of information are consistent with the ICAC criteria referred to above. Policies for the release of information are classified according to the nature of the information sought and the type of individual or organisation seeking the information. Thus, policies relate to:

- Information sought by members of the public about themselves;
- Information sought by members of the public and outside organisations about other people;
- Information sought by members of the public and outside organisations about particular circumstances and incidents;
- Information sought by the media for public broadcast;
- Information relating to statistics and trends sought by community groups and other organisations;
- Information sought by other government departments and agencies;
- Information sought by other police agencies;
- Documentation produced to courts;
- Information required by Police Service personnel about themselves; and
- Information released to the public seeking assistance in solving particular crimes.

New procedures related to each of these policies have recently been drafted to ensure that police are aware of their responsibilities with respect to the release of information, and act in accordance with established policies.

So how does this all work? What happens if police receive a request for information on an individual's criminal history, for example?

All requests for criminal histories are referred to the QPS Information Bureau. If an individual is requesting information on their own criminal history, then the criminal history details are released to that individual, on verification of the individual's identity and payment of the set fee (currently $33.50). If an individual or organisation (excluding law enforcement agencies) requests details of another person's criminal history, then that information is provided only if there is a statutory requirement to do so, or the release of information to the third party has been authorised by the person to whom the history relates.

Thus, if an inquirer (e.g. an employer) requests advice on the criminal history of an individual (e.g. a potential employee), that information will not be supplied without the consent of the individual concerned. In practice what normally occurs, is that the inquirer obtains the written consent of the individual prior to requesting the criminal history from the QPS Information Bureau. If there is no criminal history, the QPS responds directly to the inquirer. If there is a criminal history on record at the Information Bureau, this record is sent directly to the individual who has an opportunity to verify its contents, and decide whether or not to disclose it to the inquirer.

The QPS will protect the confidentiality of the name and address and associated personal details of any person held on record, except where disclosure is considered necessary in the discharge of law enforcement duties or normal administration of justice. The QPS will also release information to other government agencies where access to this information is connected to the legitimate functions of those agencies.

Members of the public may seek information about a particular incident or offence from police, but this information will be supplied only after reference to the particulars of any person have been removed, and reference to any proposed actions or opinions have been deleted. This information will, of course, only be provided where its disclosure is not likely to compromise or prejudice any investigation.

With respect to the release of information to the media, police recognise that the media have an important role in providing news to the public and can be of great assistance to police. However, police cannot give information which would prejudice a fair trial or in any way or interfere with the administration of justice. Once someone has been charged with an offence, only their gender, age, suburb of residence and charges may be released to the media. Other details of the investigation must come to light in court, not in the media as this may prejudice a fair trial.

Details of court cases are not released by police, but can be obtained from the court or Clerk of the Court. The previous criminal history of a person wanted for questioning over a particular incident is not released to the media. Names of suspects are never released to the media, except where a warrant has been issued for a person's arrest and/or they are considered a danger to society. Names of minors who are either offenders or victims are not released, and addresses of victims are never given to the media unless the victims have expressed a wish for this to occur.

Besides defining what information is publicly accessible, and making this information readily and cheaply available, police have a responsibility to properly protect confidential information.

The QPS uses a number of methods to protect confidential information. Policies and procedures define how police should protect information, and the Code of Conduct includes a description of the type of behaviour and attitudes which police should have with respect to the use of information. Police receive training in these areas, and their information management practices are subject to periodic inspection, scrutiny, and review.

Police access to information is controlled according to their operational requirements and responsibilities. Thus, not all police have access to all information. Access is defined on a "need to know" basis.

Police computer systems are protected by an extensive range of security arrangements, including a sophisticated and effective transaction logging system. This system is used to identify inappropriate use of computer systems, and it can also be a useful investigative aid for police.

There is always room for improvement, though. The QPS is currently revising its information security arrangements in response to the recent Public Sector Management Commission (PSMC) Review of the Service. The ICAC Report on Unauthorised Release of Government Information emphasises the value of computer security cards to augment recognition systems such as passwords and user identification numbers. These would certainly improve security, as would increased use of software and data encryption. However, these enhancements come at a price, and often have to compete with other government and operational policing priorities.

Recent interest and debate on privacy issues and public access to information have helped government agencies focus more clearly on their responsibilities as custodians of government information. The ICAC Report exposed the extent to which unauthorised release of government information was occurring, and helped clarify some of the main causes of the problem. The QPS has responded by

thoroughly revising its policies and procedures on the release of information. The Service will also progressively introduce more advanced techniques and technology to ensure the protection of confidential information well into the future.

CHAIR: Thank you, James Hann. Our next speaker is Dr Nicholas Chantler, from the School of Information Systems at the Queensland University of Technology.

Nicholas Chantler has a background in education, electronics, telecommunications, computing, agriculture and the military. Prior to his current position as lecturer at QUT, he was the first Head of Computer Security for the Australian Regular Army from 1989-91. He is still connected with the military, as an Intelligence Officer (Counter Intelligence) in the Army Reserve at the School of Military Intelligence, Canungra. Nicholas Chantler is currently completing post-graduate studies involving research into computer hacking. He is the author of many papers on the subject, and is considered a leading authority.

Dumps to Dipping and Weekend Markets by Nicholas Chantler

Abstract

The paper deals with the deliberate or inadvertent, unlawful release of government information, associated with computer based information systems.

The paper considers:

- how sensitive information finds its way into the wrong hands
- the methods that hackers use to find information
- the type of information that is available on the CU (Computer Underground)
- recent case histories
- indicators of hacker activity on computer systems
- the Australian scene.

The information that is found away from its environment can be used as an indicator of which government departments may have a security problem.

Introduction

This paper reflects the author's involvement in the *Protective Security of Automated Systems* (computers/information systems) and an area of research over the last nine years, an ethnological study into *The World of the Computer Hacker The Computer Underground (CU): Cyberspace.*

Some examples of hacker groups whose alleged activities have reached the press include:

- the Legion of Doom, a vindictive group who jammed the emergency telephone lines across several states in the US, with the intention of planting viruses to disrupt operations

- the Chaos Computer Club, which stole several billion dollars worth of research programs and hacked into French space and atomic energy systems

- the 414 Gang, who broke their way into US defence systems and modified medical research systems

- the Data Travellers, who penetrated more than 135 systems worldwide via NASA's SPAN network to gain access to top secret information.

Hackers communicate by means of bulletin boards which they establish either on a personal computer with a modem, or on an unsuspecting organisation's system. Bulletin boards "owned" by specific groups are heavily secured against access by other hackers. The more public ones are used by hackers generally to trade information, software and stories of successes and problems.

Bulletin boards contain software giving information on making explosives, phone phreaking, traversing international telecommunications networks, credit card fraud, writing viruses and many other sordid topics. In the main, hackers trade information; however, many also barter information for equipment or money, depending on their motive.

The paper considers:

- how sensitive information finds its way into the wrong hands
- the methods that hackers use to find information
- the type of information that is available on the CU (Computer Underground)
- recent case histories
- indicators of hacker activity on computer systems
- the Australian scene.

How sensitive information 'escapes' into the wrong hands

Sensitive information, in this context, is defined as corporate government data. Just because it is labelled as "sensitive" does not mean it is classified data. However, classified government data does find its way into the public arena, as I shall make mention of later.

Information can "escape" from its "home-environment" in the following ways:

Deliberate Disclosure

The disgruntled employee who "couldn't care less" or who is "out to get even" may actively supply information to bring about a bad image on a person or department.

The computer hacker who believes in the ethics of "open-information"; that is, "if it is on the system, it is fair-game"; after all the greeting screen *does* say 'Welcome – please login now.'

The consultant who is employed in industrial espionage. It is interesting to note at an EDPAA conference in the US, a presentation described how there is a shift away from military and political targets by FIS (foreign intelligence organisations) to the industrial technology of other countries.

The thief ("contractor"?) who needs to get the government information so that they can present more competitive prices to win "the toilet-roll" tender.

The political activist who sees information that would be of great benefit to their party or to an ideological future. Leaking information to the press is already a well-known activity.

Inadvertent Disclosure

Poor security procedures:

- poor disposal procedures of computer "waste", sensitive printouts to the local tip (DUMPS)
- poor access controls allowing anyone into the office
- terminals logged on, when away at lunch time
- information left lying around for visitors to see
- diskettes left out/taken home
- printouts disposed at primary school for art-work, with sensitive information on the "back"
- poor maintenance procedures, replace "failed" hard-drives
- computers sold with sensitive information on them
- information left in phone boxes, on buses or just "lost"
- discussions in the wrong place, cafes and bars etc.

Methods used by hackers to find information

Hackers use a variety of methods to gain access to and manipulate computer systems. However, all hackers need to successfully login using a legitimate user name or account and password to penetrate a system. Hence the key for a hacker is obtaining or guessing valid account information.

Hackers look for *inactive accounts* to use. On entering a new system, accounts that have never been used or not used for a period of time are ideal for hackers to access and claim. By changing the password and security level, a hacker is able to come back to the system at a later date at superuser level via the newly acquired account.

Some systems are designed to establish new accounts with a default password, such as PASSWORD, or some form of the user's name. New users do not always access their accounts immediately they are created, in fact, some seldom or never access their accounts at all. Such accounts are easy for hackers to identify and guess the default passwords assigned. An additional problem is that many users never change their passwords and so accounts remain with the default password originally assigned by the system.

In order to remember passwords, users often write them down or use common words. Some of the most common passwords used are PASSWORD, SECRET, SEX, LOVE, name of user or relative,

name of car or family pet, nine spelled backwards. or an easily guessed pattern. System administrators often use the password GOD. Hackers try these common patterns and combinations when attempting to gain access.

Operating systems for mini and mainframe computers usually have default accounts with different levels of access established before installation. Each system is modified on installation to suit the organisation's processing needs, and in many cases these default accounts are not removed on system set-up. Hackers know the default usernames and passwords and gain direct access at numerous levels to these systems.

As a further method of obtaining user account names and passwords, hackers frequently write programs to mimic the login procedure of systems where they desire access. This decoy program is then directly run from the automatic execution file called on initialisation. The mimic program then copies the user's login data, i.e. username and password, to a separate file, and gives the user a message such as Invalid Username – Please Try Again. Control then passes to the true login program and so the user gains access with little suspicion.

The *decoy program* is sometimes called a "trojan horse", i.e. illegal code which executes while the computer is also running a legitimate program. There is usually no evidence of the activities of the trojan horse program at the time it is running, and hackers erase evidence of the code once it completes the desired task.

To acquire more information about an organisation, its employees and its systems, hackers use two main methods, *Social Engineering* and Garbology. Social

Engineering is getting information from someone by pretending to be someone else (Clough and Mungo, 1993:66). Hackers undertake such personal research by *masquerading* as privileged employees, students conducting surveys, technicians doing repairs, and the like. Garbology is rummaging through garbage bins associated with company offices looking for written information; it is sometimes also called *dumpster dipping,* (DIPPING) dumpster diving or trashing. Scavenging from rubbish bins has been used in known cases of credit card fraud (Fitzgerald, 1992) and blackmail (Chantler, 1992) in Australia. These methods allow hackers to compile considerable information from telephone calls, written material, observations and questionnaires, which they then put into action in their illicit activities.

The majority of hackers learn to program in BASIC as their first language due to its simplicity and availability on PCs. The PEEK and POKE commands in BASIC enable the programmer to *read data held in memory* and alter it. This allows hackers to read log-on information in memory and to change levels of authorisation once in the system.

A system will generally hold a command in a buffer while it checks the user's authorisation privileges before executing a given command. In some systems it is possible to access data held in the buffer and alter the command during the short time it takes the system to verify the user's authority. This gives hackers the opportunity to enter a low-level command such as DATE or TIME, and, while the system is checking their authority, change the command to a higher-level request, one above the level of authority allocated to the account they are using.

Hackers love to find *trapdoors* allowing immediate superuser access to an entire system as these are difficult to implant into installed operating systems. Trapdoors are holes or secret doorways into operating systems which bypass the normal security controls. These allow direct access to the operating system and are put in place whilst systems are under development. Trapdoors assist the designer when testing the system, as they provide a way in at superuser level when the system fails. Trapdoors can deliberately or unintentionally remain in the finally delivered system.

Viruses and worms are *'rogue code'* often used by hackers wishing to sabotage targeted systems. A virus is a program which attaches itself to other programs. Viruses replicate by copying themselves onto other programs and disks. Using the logic bomb technique discussed below, a virus shows itself at a specific time when a predetermined action or set of conditions occurs. Viruses can be benign; however, most are damaging. More sophisticated viruses such as stealth viruses are programs which can move around in memory and avoid viral detection programs. This type uses several levels of encryption and is difficult to find and erase. Worms are complete programs that reproduce themselves by "worming" their way through networks using unused computer resources.

A logic bomb is a set of instructions activated by the occurrence of a predetermined action or event usually programmed to the system clock. Hackers use logic bombs as separate programs in themselves, or in the form of trojan horses. For example, hackers will use logic bombs to activate a program to execute during periods of low usage on an organisation's system. Logic bombs are also used to activate viruses.

The above techniques are only a few methods utilised by hackers. Further information on methods used by hackers can be found in Chantler, 1990; Cornwall, 1985; Landreth, 1989; and Stoll, 1989.

The type of information that is available on the CU

So long as the information has some appeal, either for being "different" or for being "restricted" technical, it will be found on the CU. Technical articles to do with government computer sites, military computer sites, and how to hack into the types of machines used by those organisations. Files that deal with government political issues, locations of telephone exchanges and how they work, public phones and how to bypass being charged for calls. Methods of conducting fraud against government bodies, military and police frequencies – including the voice codes they use.

Recent incidents

The HDD (hard disk drives) and weekend markets (WEEKEND MARKETS): I have a friend who fixes computer components for someone who sells them at the weekend markets.(The person he fixes them for goes around computer shops and buys their "old junk" to see if it can be "got going again"). Knowing my past military experience in computer security, he called me one weekend to say that he had found something interesting on some PC (personal computer) hard-disk drives which he was testing; he had found a recent defence (electronic) telephone directory.

It is possible to recover information from a hard-disk even after it is erased, but the information on these drives had not been erased. There were four drives and this is what they contained:

- Drive 1 – from the Department of Defence containing RESTRICTED covering CONFIDENTIAL material to do with political aspects of staff in neighbouring countries.

- Drive 2 – from the Department of Defence containing RESTRICTED information and policy statements do with Conditions of Service and other matters.

- Drive 3 – from a high profile businessman who deals with property. Information included all of the letters to his contacts about a new CONFIDENTIAL land and money scheme which would be of benefit to the political party members involved.

- Drive 4 – was from a security company on the Gold Coast who deals in special alarm systems. The information included a list of incomes and expenditures, staff and customer names and addresses (including details of alarm systems and repairs carried out), new circuit and printed circuit-board designs for new alarm systems developed in-house.

I wonder if those high-profile personalities involved would be happy to know that I have read mail written to them, or by them?

Indicators of hacker activity on computer systems

Unless they are extremely careful and meticulous, hackers tend to leave footprints within systems that indicate where they have been. System logs will give details of pattens of hacker movements and should be checked frequently. Some tell-tale signs of hacker activity are:

- Hackers on a system are evidenced by excessive log-on times, and the use of inactive accounts for days on end. Once they have access to a system via an account, there is a tendency to utilise this facility to the maximum whilst access remains. Hackers prefer to work through the night when fewer users are logged-on. This gives quicker response times and offers less chance of being detected. Hackers also tend to use given pattens when traversing systems. They move extensively throughout the system and carry out activities which are generally outside the normal activities of the user they are imitating. Hence, system logs showing unusual local times of activity, activity on inactive accounts and extensive movement around a system's facilities are indications of hackers.

- Source files are of special interest to hackers who want information contained in programs or data files. Object files are of little use as they cannot be modified. Hackers will establish directories and move or copy files into these directories for their use. Hence directories or files that have been moved, filtered, copied or deleted show hacker activity on the system.

- Hackers use electronic mail to keep in touch with other hackers on a particular system. The appearance of strange electronic mail messages can indicate hackers are using the computer. They also pick up vital information from reading electronic mail and will delete chosen messages if they feel threatened or if a message contains useable information.

Hackers seldom go back to change the flag which indicates whether the mail has been read. Pre-read or lost electronic mail are other signs of hacker activity.

- Hackers will set up sub-accounts in a given account through which they have gained access on large systems to enable other hackers in their inner circle to use the same system. Bill Landreth (1989) recalls situations where up to 30 hackers would use the same account. In many cases hackers will establish a bulletin board on the system in use.

- Help files are used extensively by hackers to gain knowledge of systems. Without manuals, help facilities give hackers the information they require to write successful programs on their chosen systems. Excessive use of help files can also indicate hackers are present.

- Unless a hacker has knowledge of an active username and password, he or she can only guess possible successful combinations. Programs to automatically attempt logins on systems are readily available on bulletin boards. Hackers will run such programs through the night and store successful phone numbers and login details. Hence an unusually high number of unsuccessful logins on a system indicates hackers attempting to gain access.

The Australian scene

How vulnerable are we, in Australia, you may ask? Research carried out at Queensland University of Technology as reported by Simmons (1993) in *The Australian* of May 18, reveals that Australia has one of the highest levels of computer literacy per capita. This research also suggests that Australia is being used by hackers overseas, to break into sensitive computer systems in other countries (through Australian based computer systems) due to our lax computer security.

At one time, Australia had more radio hams and private pilots per capita than any other country; probably due to our geographic isolation. For much the same reason, hackers are numerous and very active in Australia. Our hackers use the same bulletin boards, tools and techniques as hackers elsewhere in the world. Our isolation could be seen to encourage such global communications activities.

For Australian organisations, an essential key to minimising the abuse of unauthorised access is the awareness and education of personnel within the organisation itself. The development of global networked communications has opened up an entirely new sport for those who are bright and motivated. However, hacking is no longer just teenagers at play; it is an illegal activity undertaken by a great number of people who vary considerably in ability, stability and ethics.

Organisations relying on networked systems are threatened by hackers solely because of the nature of those systems. The risks of abuse by hacking are rising and the implications are severe. Cyberpunks, the new breed of hacker, jack themselves into corporate and government computer systems, navigating their way through networks of classified and highly valuable information.

Summary

The risk of losing information is high. This is due to the poor protective security measures which are afforded in some government departments. Security has always been the thorn in the side of management. Perhaps this is why we choose to turn a "blind-eye" to it.

The major threat may be internal or external, with a range of personalities involved: from lazy worker to the hired consultant; these areas are where the greatest risks exist.

Whilst I have mentioned computer hackers at length, I do not believe that they are the major risk. It is true that a risk must exist from them, for they are very organised, they determine the direction which they want to pursue, they collect and collate information and then disseminate it. (Those of you who are familiar with the Intelligence Cycle will recognise that hackers also use the same system.)

It is interesting to see the information within the CU as it gives those of us in security an indication of which departments may be rather lax on security.

REFERENCES

Chantler, A.N. (1990). 'A Description of Different Types of Rogue Code'. The Australian Computer Abuse National Conference, 29-30 November, Gold Coast, Queensland.

Chantler, A.N. (1992. 'In your Competitors Shoes'. ACS Seminar, Perth.

Clough, B. and Mungo, P. (1993). *Approaching Zero* London: Faber and Faber.

Cornwall, H. (1985). *The Hackers Handbook* UK: Century Communication.

Fitzgerald, K. (1992). 'Credit Card Scam Run by Schoolboys'. *Computer Control Quarterly,* Volume 10, No 1, p. 61.

Landreth, B. (1989). *Out of the Inner Circle*, 2nd ed., Washington: Tempus Books.

Simmons, C. (1993). 'Hackers Trade on Terrifying New Ground'. *The Australian*, May 18, p. 16.

Stoll, C. (1989). *The Cuckoo's Egg.* Great Britain: Bodley Head.

CHAIR: Thank you, Nicholas Chantler.

The next speaker in this session is Mr Kevin O'Connor, Privacy Commissioner of the Human Rights and Equal Opportunity Commission.

Kevin O'Connor QC is the first Federal Privacy Commissioner and has held that position since the commencement of the *Privacy Act* in January 1989. He is responsible for implementing federal privacy laws. With degrees in law from the Universities of Melbourne and Illinois, Kevin O'Connor has had a career as an academic, a barrister and a senior public servant From 1976-1979 he worked with the Australian Law Reform Commission, and was heavily involved in research for the Commission's major report on privacy. He has also been a member of the Australian delegation to the United Nations Commission on Human Rights on three occasions.

Thank you for the opportunity to speak with you today. The unlawful release of government information is a subject which has received a great deal of attention in recent times. As such, I consider this conference a good opportunity to give you an overview of the current state of Commonwealth law and thinking in this area.

By way of introduction, I think it would be useful if I clarify my role and jurisdiction as Privacy Commissioner. I will describe the way in which the federal *Privacy Act* impacts on unauthorised disclosure of Government information, with particular emphasis on computer based information. I will then outline other Commonwealth legislation affecting unauthorised disclosures. I will also give a brief update on a major Government inquiry which has relevance for today's discussion.

Role of the privacy commissioner

As Privacy Commissioner, I have responsibility for administering the federal *Privacy Act*, which was passed in 1988. The main thrust of this Act was to apply a series of Information Privacy Principles (IPPs) to the Commonwealth public sector. The Act requires federal Government departments and agencies to comply with eleven IPPs. They govern:

- methods used to collect personal information
- storage and security of personal information
- access by individuals to their personal records to ensure accuracy of those records
- use of personal information and its disclosure to third parties.

For the purpose of today's discussion the two most relevant IPPs are IPP 4, which requires agencies to implement security safeguards to protect personal information, and IPP 11, which sets limits on the disclosure of personal information by agencies.

Under the Act, I have the power to investigate complaints by individuals who believe that their privacy has been infringed due to a breach of the IPPs.

It should be noted that the IPPs govern acts or practices of Commonwealth agencies. Accordingly, the Act does not provide a remedy in all cases of unauthorised disclosure by Commonwealth officers. It may be that the officer was

acting in his or her personal capacity and in contravention of departmental policy. However, the action may well constitute a breach of IPP 4, which relates to storage and security of personal information by the agency. This would apply where the disclosure was made by someone who was not authorised to handle the information in question.

In addition to the IPPs, section 27 of the Act gives me a broader role of undertaking educational programs to promote the protection of individual privacy. This aspect of my jurisdiction applies not just to Commonwealth agencies but to state bodies and the private sector. Unauthorised disclosure is one of many areas which I sometimes address in this role.

Corrupt disclosure of personal information

The ICAC inquiry has given a depressing insight into the culture of disregard for individual privacy that is found in many investigative and security wings of private and public organisations. While ICAC's investigation was, naturally, focussed on information held by NSW Government agencies, it is reasonable to assume that the practices described occur nationwide and involve officers at all levels of government. In the case of Commonwealth administration, ICAC found examples of trade in protected information involving officers of the Department of Social Security, the Australian Customs Service, the Department of Immigration, the Health Insurance Commission, the Australian Taxation Office, the AFP, the Australian Postal Corporation and Telecom. Systems based on bribes and the exchange of favours have given rise to serious breaches of individuals' privacy. Address information is not a trivial item of information. Nor are telephone number details or other locater data. For most people these are highly sensitive items. All people who commit their data to government (or private) organisations are entitled to have their expectations of privacy respected in the way their data is handled. Organisations should have clear and explicit policies on how individual data are handled, and their policies should be known to those with whom they deal.

Commonwealth response to ICAC inquiry

Following the release of the ICAC Report in August 1992, I contacted all Commonwealth agencies adversely mentioned, and asked them what action they had taken in response to the evidence when it was first aired, and what if any further action they were taking in response to the report. I also enquired as to the changes in security practices that had flowed from the report. (Telecom were not contacted as they are not covered by the *Privacy Act* and are therefore outside my jurisdiction).

In the case of *Australia Post*, several employees had been named in the transcript. I was advised that three employees identified in ICAC left employment during a

joint Aust Post/AFP inquiry into information handling practices in NSW. This inquiry arose after the Manager, Security and Investigations Unit received information that certain officers from that unit may have been involved in the unauthorised release of information. This inquiry was unable to adduce sufficient evidence to support criminal proceedings.

Four officers identified in ICAC are still employed by Australia Post. Aust Post state that interviews of those officers have now been conducted and their investigations are expected to be concluded shortly. Aust Post state that they will take appropriate criminal or disciplinary action dependent upon the results of their investigations.

Since ICAC Aust Post has reminded all staff of their obligations under the *Australian Postal Corporation Act* 1989 and *Crimes Act* 1914. Local training includes reinforcement of these issues. The *General Procedures Manual* contains references to expected standards and penalties.

Australia Post state that all requests are now to be in writing to be considered by the relevant liaison officer. Only urgent requests (police etc) will be processed otherwise and a record is kept and audited by the managers of the relevant areas.

In the case of the *Australian Tax Office* (ATO), the Office advised that there was no evidence of ATO information being leaked. The ATO state that the only mention of the ATO was an allegation that some names and addresses obtained by an enquiry agent were passed from a tax officer to a prostitute (who was subsequently murdered).

The ATO have formed a National Security Committee chaired by a Second Commissioner. An ATO security manual and a Code of Ethics have been issued. A dedicated computer security section is now in place.

In the case of the *Department of Immigration and Ethnic Affairs* (DILGEA), the Department stated that they only became aware of the identities of the persons named in evidence when my office provided them with transcripts. Since then they have conducted a detailed investigation and concluded that their departmental officers did not knowingly breach Commonwealth law. They provided a copy of a detailed investigation report, and this conclusion seems reasonable.

Training for all departmental officers has increased as a result of ICAC. Staff news and other departmental publications have publicised these incidents to increase awareness. The Department provided a detailed submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs: Inquiry into the Protection of Personal and Confidential Information Held by the Commonwealth.

In the case of the *Department of Social Security (DSS)*, of the 37 staff who gave evidence at ICAC or were named by third parties, all but two denied any wrongful release of information. In January 1991, the Australian Federal Police investigated the 37 staff and referred 36 cases to the Director of Public Prosecutions. The DPP considered that a prima facie case existed in two instances.

DSS advised me in November 1992 that one individual was found guilty on 13 August 1992 of an offence under s.19 of the *Social Security Act*. Fined $400, recog in the sum of $1,000 to be of good behaviour 12 months. He had been suspended from duty without pay since 27 May 1991. Disciplinary action was to be taken.

The other officer was charged on 18 May 1992 with a similar offence. This matter was adjourned until February 1993 for committal. The matter is still waiting to be heard. The officer was suspended with pay from 6 March 1991 and without pay from 1 June 1992 after formal charges.

Since ICAC, DSS has circulated numerous instructions to staff and an internal privacy audit has been conducted. A privacy awareness kit has been issued to all staff as a result of ICAC and a security awareness campaign has been launched.

In the case of the *Australian Customs Service* (ACS), the ACS stated that in early February 1991, they became aware that officers were being named in ICAC and were to be called as witnesses. ACS investigation revealed that officers in ACS Regional Intelligence Unit in Sydney had been providing information on a reciprocal basis for a number of years. On 13 February 1991 an instruction was sent to all ACS regions reinforcing secrecy provisions (s.16 *Customs Act*) and the provisions of the *Privacy Act*.

Four officers admitted to ICAC that they released RTA information, which they had access to, to electricity authorities in exchange for habitation checks. One officer admitted releasing electoral information on the same basis. Payment was denied. Immediately after, each officer was counselled. Aust Govt Solicitor advice on 27 June 1991 was that disciplinary action was not warranted. ACS were written to again on 27 October and given the names of four other officers named in the transcripts. ACS replied on 9 November 1992 that three had left ACS employment before the commencement of ICAC and no action has been taken. The fourth officer was counselled in the same terms as the previous group. ACS stated that it had sent out two staff circulars and that training has now been integrated into a range of ACS courses. They state that new computer systems with enhanced audit trail capacities are currently being installed. There is also a warning on the computer screen in relation to access.

In the case of the *Health Insurance Commission* (HIC), two officers appeared before ICAC and admitted releasing information contrary to the *HIC Act*. Both

officers were suspended in January 1992 and their statements referred to the AFP. AFP prepared briefs which were submitted to DPP. At that time, DPP had yet to decide whether to prosecute.

HIC were written to again on 22 October 1992 for an update. They replied on 17 November that in relation to the first officer, the DPP advised it does not propose to take criminal action. In relation to the second officer the AFP did not propose to recommend prosecution. Both officers have been charged by the HIC with failing to fulfil their duty. They have been suspended and an independent officer has been appointed to determine the matters. HIC stated that 67 internal audits have been conducted since January 1992; specific areas included security and mail room procedures.

The AFP advised in December 1992 that investigations into the officers named are still continuing. There has been a steering committee appointed to review computer security and a computer security training course devised. They stated that measures have been taken to further limit access by some users and they have a screen message regarding members' statutory responsibilities. They state that a computer audit trail is in place and is publicised throughout the AFP. 30 computer audits have been conducted in the last 6 months. The AFP formed an Internal Security and Audit Division in April 1990. Verbal advice in late August 1993 from AFP indicated that Internal Investigation Division has completed investigations and will provide a report shortly.

My auditors have formally audited aspects of the systemic practices of several of these agencies, and have not found any systemic problems which might contribute to corrupt disclosure. They tend to see the issue as one of officer ethics, as inferred by the agency's culture and environment.

Major Audit of Department of Social Security: The Australian National Audit Office in July 1993 began a large scale audit of practices at DSS, in relation to the protection of confidential client information from unauthorised disclosure. The audit is expected to continue for several months.

Inadvertent disclosure of personal information

Besides corrupt disclosure, there is the problem of casual or inadvertent disclosure. The individual can often be hurt more by a disclosure made after work over a beer than by one which arises from a systemic failure, such as a mail-out error, or a corrupt disclosure. Often the casual disclosure is made to someone who knows, and who may have a special relationship with the individual affected. My office has had occasional complaints of: gossiping with colleagues at the pub after work about sensitive case material; or an officer passing client information to his or her spouse. Disclosures of this type could also be indicative of inadequate security

safeguards by the agency employing the officer to protect the confidentiality of personal information.

Information security and computer technology

As I mentioned earlier, IPP 4 requires that reasonable security measures be implemented for protecting the confidentiality of personal information. The need for such security measures has assumed a greater significance with the spectacular advances in information technology and the growing predominance of computer records as distinct from data held in paper form. This is because of the huge amounts of data able to be held in computer form and the ease with which they can be accessed, reorganised, manipulated or transmitted. Many large organisations have mainframe systems for managing data linked to large numbers of terminals throughout Australia.

Security is a relevant factor when an organisation is choosing its computer equipment or software. The level of security chosen obviously depends on the extent of the risks seen by management as likely to affect the data balanced against operational needs. Some deficiencies in security measures implemented by various Commonwealth agencies identified by my office include:

- absence of automatic log-off or automatic screen shutdown
- lack of facility for enforced password changes
- failure to delete the access facility for retired employees.

Deterrents against unauthorised disclosure

The ICAC Report emphasised the importance of logging of users' transactions and enquiries on computer systems for audit and usage investigations, and to deter misuse. My office's experience strongly supports this conclusion. Investigation of alleged disclosures of protected information are liable to be severely hampered unless there is an adequate audit trail. Access records also allow agencies to conduct internal monitoring of staff access to records. Checks of this sort, conducted on a regular basis, are strongly recommended as a means of both deterring and detecting improper access to information, but obviously rely on adequate information about usage being collected.

Experience to date indicates that many agencies do not maintain satisfactory records of access. In considering what records are adequate, both the amount of detail recorded about each transaction or enquiry and the retention period are of importance. Most large scale operating systems include a facility to record date, time and duration of access and user identification. For the purpose of effective

privacy protection, it may also be necessary to record the nature of the enquiry or transaction and even, in some cases, the actual output or result of the enquiry.

Some agencies maintain user access logs but keep them for only short periods. As there is frequently a delay of several months between a possible unauthorised disclosure and the matter being the subject of a complaint, logging information needs to be retained for a significant period, at least 12 months, if it is to be an effective investigative tool.

Commonwealth laws affecting unauthorised disclosure

I have endeavoured to give you a feel for the *Privacy Act* and the IPPs, as they relate to unauthorised disclosures, particularly in the context of computer based information. I will now give you a brief overview of the state of Commonwealth law in this area, beyond the *Privacy Act*:

(i) Penalties for Unauthorised Disclosure

Commonwealth officers who corruptly disclose protected information are not currently subject to any proceedings under the Privacy Act which, as I have already explained, deals with acts and practices of agencies rather than individual officers. They may, however, be liable to a range of penalties under criminal and disciplinary provisions including the following:

Public Service Act discipline provisions – under s. 52 of the *Public Service Act*, an officer employed under the Act may be disciplined for failing to fulfil his or her duty, following an inquiry conducted by the agency. Penalties range from a fine of up to $500 to dismissal.

Crimes Act provisions on unauthorised disclosure – of most relevance is s. 70 of the Act, which makes it an offence for a Commonwealth officer to disclose information obtained by being an officer where there is a duty not to disclose. The penalty is two years imprisonment. "Commonwealth Officer" includes all those employed under the *Public Service Act*, and other major categories, including the Territory Public Service, the defence forces, Commonwealth public authorities, the AFP, Australia Post and the Australian Telecommunications Corporation.

Unauthorised access – s. 76B of the *Crimes Act* also makes it an offence to intentionally gain unauthorised access to data stored on a Commonwealth computer. This provision could apply either to officers of an agency who obtained information by means of unauthorised access, and subsequently supplied it to outside parties, or to outside parties who accessed information directly from an agency's computer. Amendments to the *Social Security Act* were recently introduced to make it an offence for any person, including an officer, to access

social security client information without proper authority or to disclose or deal in information obtained by means of such access.

Secrecy provisions – many (but not all) Commonwealth agencies are covered by secrecy provisions, which make it an offence for an officer to disclose information held by the agency without proper authority. The terms and penalties of these provisions are various. It is understood that the Attorney-General's Department has been examining the secrecy provisions of Commonwealth agencies for some time.

- other provisions – staff of Commonwealth bodies not employed under the *Public Service Act* may also be subject to disciplinary provisions covering unauthorised disclosure of information.

Clearly many of these provisions run in parallel. The same disclosure might be subject to disciplinary proceedings, and prosecution under the *Crimes Act* and the relevant secrecy provision.

(ii) Penalties for soliciting unauthorised disclosure

Up until now, penalties for unauthorised disclosure of confidential information have focussed almost entirely on the errant officer. Provisions have recently been included in the *Social Security Act*, the *National Health Act* and the *Health Insurance Act* directed at the procurers, making it an offence, punishable by two years imprisonment, to seek unauthorised disclosure from officers of the agencies covered by those Acts. It remains the case that the parties who solicit unauthorised disclosure of information from agencies other than those mentioned do not commit an offence.

In my first and second annual reports I proposed that the Government should consider amending the criminal law, to enable those that are parties to corrupt disclosures to be prosecuted and possibly to place some direct liability on the principals. This proposal was based on the perception that the trade in confidential information depends on the existence of willing purchasers. I also proposed some extensions to my powers to enable investigation of all the circumstances of incidents of unauthorised disclosure, including activities of those procuring information by these means, and award damages against those who procure unauthorised disclosure of information.

This view seems to have been reinforced by the findings of the NSW ICAC. The typical pattern of activity detailed by the ICAC report is of information being obtained in the first instance by intermediaries such as private investigators, but with the end users being corporations in industries such as the finance and insurance industries. The report emphasised the necessity of attacking this process 'at every point on the distribution chain', and recommended that unauthorised dealing in protected government information be made a criminal offence.

In June 1991 the Senate Standing Committee on Legal and Constitutional Affairs provided a limited response on the matters I raised in my first and second annual reports. However, to date this has not involved any significant changes to my investigative functions as proposed.

Recent Developments

Having given you an overview of the current state of Commonwealth law affecting unauthorised disclosure of Government information, I will now update you on some more recent developments.

In August 1992 the House of Representatives Standing Committee on Legal and Constitutional Affairs commenced an Inquiry into the Protection of Confidential Information Held by the Commonwealth. The Inquiry has broad terms of reference including the adequacy of administrative measures for safeguarding third party information, legal safeguards for third party information, and the adequacy of mechanisms for dealing with unauthorised disclosures of information.

In October 1992 I made a submission to the Inquiry. My submission considered, among other things, mechanisms for dealing with unauthorised disclosure of personal information and soliciting of such disclosure, and for providing redress to individuals about whom information is wrongly disclosed. My recommendations included the following:

- That broad penalty provisions be established relating to the soliciting, either directly or indirectly, of unauthorised disclosures of personal information held by Commonwealth bodies. Such provisions could be included in the *Privacy Act*. Consideration could also be given to including an offence of dealing in personal information obtained through unauthorised access.

- That the *Privacy Act* be amended to allow me to impose liability (in damages) on those who procure the improper disclosure of personal information.

- That my powers to investigate unauthorised disclosure of personal information be extended to allow investigation of all aspects of the disclosure including the actions of parties who, directly or indirectly, obtain personal information as a result.

- That in cases where my investigations under the *Privacy Act* lead to the possibility of criminal prosecution, my investigative functions be extended to include development of the prosecution case by arrangement with law enforcement authorities or the Director of Public Prosecutions.

In October 1992 the Attorney-General's Department also made a submission to the Inquiry into the Protection of Confidential Information. The Department indicated general agreement on a number of issues on which I commented in my submission.

Conclusion

In conclusion, I hope I have conveyed to you not just the formal legislative framework affecting unauthorised disclosure of information, but also, in a broader sense, the importance of organisations taking security of personal information seriously. The breaches of security associated with unauthorised disclosure of personal information have potentially dire and far reaching consequences. They place at risk significant national interests such as law enforcement or economic regulation, and erode public confidence in organisations' respect for the rights of the individual. The difficulties of protecting against unauthorised disclosures will increase as technology advances and society comes to depend more on the free flow of information. I believe it is vital for these issues to be kept at the forefront of public debate on information privacy. To that end, I regard this conference as extremely worthwhile, and I thank you for your time.

QUESTION AND ANSWER SESSION

Kelly — Thank you very much Kevin. We now have some time for questions. Unlike our previous Chair I would encourage you to state your names and the organisations you represent. Can we have some questions please?

Question 1 — Nev Garnham from Gold Coast City Council. Mr O'Connor, in your jurisdiction you have the *Freedom of Information Act* and *Privacy Act* seemingly going hand in hand, but what would you say about the fact that Queensland has a *Freedom of Information Act* that is very much missing a *Privacy Act*?

O'Connor — Well as you probably appreciate it's not really good policy for Commonwealth officials to start making observations on what state governments should or should not do so I don't propose to do that but obviously I see value in legislation whether in Queensland or anywhere else in Australia looking actively at developing privacy laws. Queensland did put out a discussion paper in 1991 which raised this question, but it hasn't led to any further policy announcement. The New South Wales government made a policy announcement in December 1992 to the effect that it was introducing data protection legislation but the bill that has been promised now for some time hasn't surfaced in the New South Wales Parliament and I understand that there's still debate going inside government administration in New South Wales as to the scope of that Bill. But nevertheless you can see from those examples that some interest is now being shown at state level.

I think that the conundrum is really the one that I've raised previously. Where the debate really lies is the extent of legitimate dissemination of data within an agency setting or a business organisation setting and similarly, the extent of legitimately disseminating data beyond that setting. And then once you decide what's legitimate in terms of dissemination practices I believe you then get into a fairly complex discussion about tiered safeguards.

There are some forms of dissemination that ought not to be like the subject of undue bureaucracy but there are other levels of dissemination of data that raise fundamental public interest issues and need to be the subject of wide knowledge as to their occurrence and fairly detailed disciplines as to when they occur. Of

course I'm referring in that regard to data matching, matching of entire databases as between difference agencies.

So what we have to do in Australia at the moment is to get down and say what are the permissible dissemination practices and what aren't. The debate isn't so much around the other issues. But there's no doubt that State Parliaments are following the federal development with interest and some have gone part of the way down the track. South Australia has administrative instructions in the form of the information privacy principles applying to its administration. The ACT is on the verge I think of passing its own Privacy Act. New South Wales has made a policy commitment to the effect that it will have such an act.

New Zealand interestingly passed an act in the last year which binds the New Zealand public sector immediately to a statement of principles like the Australian IPPs and also applies specific standards to the use of identification numbers and data matching. Then it gives the private sector three years to develop codes of conduct which have the approval of the New Zealand Privacy Commissioner and basically respond to the principles that I've referred. And if at the end of three years they don't have any approved code in place they simply fall subject to the general principles which in many instances would be worse. So there's a phase-in for private sector coverage occurring in New Zealand.

The discussion is one that will over the next several years lead to there being some form of data protection law in most parts of the country. There'll also be a debate about extension of the federal law beyond its current parameters.

Question 2 Isn't it really a matter of appropriate balance and what you think about the public interests and the protection of the individual? For example the media should not give publicity because they go beyond the bounds of privacy, and governments aren't using information correctly. Or take the case of bankruptcy when many other innocent people are affected because you don't get the proper information. Why should the criminals get the protection – the balance seems to be wrong. If only the individual can apply for information about themselves that would stop the media printing that sort of information and reduce the number of people harmed.

O'Connor Look, obviously balance is the most used word in the privacy discussion. We're always talking about the balance of interests. The

community on the one hand prizes confidentiality of relationships and also confidentiality of the information that's furnished in those relationships. Very important social values are served by respect for privacy and respect for confidentiality. On the other hand there's obviously important community value associated with a whole lot of collective pursuits whether they have to do with statistical research or research into issues having to do with protecting the community against organised crime or particular crimes of violence or robbery or whatever. Similarly in the commercial sector breaches of contract and absconding on debts can have dire results for honest consumers in terms of interest rates.

I recognise all these points of view. The hard task of Parliaments is to grapple with that balance and to define distinctions. This was left to the courts in the past and they came down pretty hard on the side of confidentiality for relationships they regarded as important and let the rest go. Parliaments have tried to be a bit softer than the courts by generalising the protections across all relationships.

What you see in the federal *Privacy Act* is really two approaches to the matter. One is a light bail through commonwealth administration by way of IPP tenants, though you'd think it was a ton of bricks when you talk to them. On the other hand the credit industry under part 3(a) is much more like a ton of bricks. That's a highly specific and detailed form of regulation.

I tend to think the answer lies somewhere between those two approaches but in the *Privacy Act* you've got the Parliament within the space of a couple of years looking at a range of conflicting interests issues and coming up with a generalised recipe for Commonwealth administration and a highly detailed recipe for the credit industry as it relates to consumer credit reports. There's no easy answer but I don't think the answer lies simply in the judgement of data managers as to what's appropriate or the judgement of police as to what's appropriate and so on. The standards have got to be set independently of that and there's got to be some kind of mechanism for protecting individuals that is independent of those interests.

CHAIR: Well that brings us to the end of our allotted time. On your behalf I would like to thank our three speakers for a very interesting and informative look at this question of the use and misuse of information from three entirely different view points. I'd ask you to show your appreciation in the usual manner.

SESSION 3

A Private Enterprise Response

CHAIR: Lewis Wyvill QC
Commissioner
Criminal Justice Commission

CHAIR: Ladies and gentlemen, the third session of this seminar looks at the problem of the release of government information from a different perspective. The speakers you will hear now are in the category of what we might call "information seekers" – those people in responsible sections of private industry who feel that in the interests of fairness they *need* access to more information about their customers and potential customers than is readily available. Mr Graham Jones is from the Insurance Council of Australia, and he will specifically address this issue – his paper is entitled "Freeing up Access to Government Information". He will be followed by Mr Chris Bishop, Director of the Legal branch of the Australian Bankers' Association, who will speak about "The Banker's Duty of Confidentiality." I'll take questions from the floor after both these gentlemen have spoken.

So let us hear first from Graham Jones from the Insurance Council of Australia.

Graham Jones, Queensland Regional Manager of the Insurance Council of Australia, has been in the insurance industry for thirty-seven years. He is a fellow of the Australian Insurance Institute and of the Australian Institute of Company Directors, a Consultant of the State Chamber of Commerce, and President of the Australian Insurance Law Association of Queensland.

Thank you for the opportunity to talk to you today. I represent the Insurance Council of Australia, which is the Trade Association of the Private Sector, General Insurance Industry. We are a representative, not a regulatory body, but we do facilitate the industry's self-regulatory initiatives and deal with proposed legislation.

To digress for a minute, the most important initiative ICA has taken in recent years has been to establish the General Insurance Claims Review Panel, which is now two years old and proving its worth. We are structured to deal with disputes and complaints and are available to assist people in disputes about breaches of privacy etc. However, out of more than 24,000 contacts we received in the last 12 months, privacy issues did not rank as an issue.

Much has been said in various jurisdictions about an illegal trade in Government information. At the outset I wish to make it clear that:

a. We do not agree with, support or condone illegal activity by public servants, or the bribery or corruption of public officials. Our industry wants to fight crime, not foster it.

b. The insurance industry in this State is keen to obtain information that may be available, but this information must be obtained through legal channels (e.g. currently we are liaising with the QPS for electronic access to the Traffic Incident Recording System STIRS).

What I do want to do is focus on the issue of privacy. It is imperative that all parties maintain a balance. A balance between the needs of our industry to deliver its service and benefits, and individuals' rights to privacy; a balance between the insurance industry's need for information to fight fraud, and thus protect the wider community, and a need for adequate safeguards.

The insurance industry provides a vital service to the community. That service and protection we provide is manifested in paying claims. We pay out millions in claims every working day with in excess of 2.5 million claims a year.

The *routine* delivery of these benefits or promises in the policies that we sell requires information. For example:

- Police reports of motor vehicle accidents or burglaries; who hit who, who was at fault etc.

- names and addresses of vehicle owners who are involved in accidents, hit and runs or who provide false information;

- Fire Brigade reports on arson.

The other side of the coin is insurance fraud. This is an endemic problem which is estimated to cost our community (that's you and me) in excess of $1 billion every year. Every fraudulent claim costs policyholders more in higher premiums. Fraud is a crime. It's not a problem that the police have the resources, expertise or even the original data to investigate. It is a job the insurance industry is doing. When we have gathered the information and evidence, we hand it over to the police, and they take it from there.

We believe that, as a matter of urgency, legislators should support efforts to contain insurance fraud, rather than opening up more avenues for abuse by dishonest members of the community.

The insurance industry needs access to data to fight fraud. The data needs to be

- readily available

- quickly supplied

- cheaply supplied

- efficiently delivered

- accurate.

We do not disagree with proper and adequate controls, informing the person, specifying the use of the data or other privacy principles as set out in the OECD guidelines. It is hoped these matters may be satisfactorily addressed to ensure that the need for any undesirable activity is removed.

To continue with fraud, I remind everyone here that affordability of insurance is a key issue, one for which the insurance industry in recent years has taken responsibility on behalf of the community. There are plenty of examples of undesirable social consequences which arise out of a vicious circle of avoidable insurance claims and escalating crime rates.

Some examples of the information an insurance company may seek from Government or semi government enterprises to validate an insurance claim are as follows:

- The Queensland Transport Department for registered owner details
- The QPS for breath analysis results, verification of accident/stolen motor vehicle and property reports
- The Queensland Rental Bond Authority for confirmation of tenant's address
- Court records for Family Law and Civil Court details
- The Registrar of Births, Deaths & Marriages for confirmation of details
- The Queensland Fire Services for fire investigation reports
- The Queensland Ambulance Service for verification of call out and accident details

These are a few legitimate requests for information.

We support a proper framework, legal, controlled and efficient for the dissemination of information for legitimate and justifiable purposes.

We support appropriate licensing or accreditation and authorisation procedures, the provision of audit trails and official inspection process. We would also make a special note of the need for uniformity of approach throughout Australia.

The issuance of data is currently under review in NSW and among other things codes of conduct are being addressed. This is an area the ICA is currently looking at by developing an industry Code of Practice. Such moves by Government agencies have the insurance industry's support.

We, in the insurance industry have a job to do in protecting the community's pool of premium from fraud and in efficiently delivering the benefits to which people are justly entitled. Provided a balance is maintained we should have no problems.

In conclusion, "the community must decide what they can afford compared with to what extent they wish to follow privacy avenues."

Finally, thank you.

CHAIR: Thank you Graham Jones. And now, from the Australian Bankers' Association, may I introduce Mr Chris Bishop.

Chris Bishop is currently the Director Legal of the Australian Bankers' Association. A Bachelor of Laws (Hons) from the University of Melbourne, he has twelve years experience as a commercial lawyer and eight years in the Banking and Credit industry, where he specialises in areas of retail credit and retail operations. Before joining the ABA, Chris Bishop was the Chief Manager, Banking Practice and Compliance in the Commonwealth Bank of Australia.

The use of Government information in relation to a bank's dealings with its customers, came into prominence with the ICAC Report on Unauthorised Release of Government Information in NSW. Discussions at this conference today principally relate to the trade in Government information and address what kind of controls should be used to safeguard confidential information of this nature and policy aspects of privacy of confidential information generally.

Australia does not have specific data protection legislation as exists in some other jurisdictions. However, as far as banks are concerned, the Federal Government Task Force Draft Banking Code of Practice released on the 18 June 1993 now specifically addresses the issue of privacy and confidentiality of information collected and used by banks.

Clause 15.1 of the Code provides:

> To the extent required or permitted by law, institutions shall observe their duty of confidentiality with regard to customers or former customers information.

Additionally the *Privacy Amendment Act* 1990 sets out the circumstances in which credit providers may disclose information contained in credit reports, personal information concerning a customer and other credit information (such as information that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity).

Information collection and use

Banking regulation initiatives

Clause 15.6 of the Government Task Force Draft Code provides:

> Institutions shall only collect information by lawful means and shall not use or disclose information which they know or believe may have been collected unlawfully.

In these lines the issue addressed at today's conference is really encapsulated in so far as the position of the banking industry in stating the policy parameters applicable.

The practical issue is of the extent of availability and collection of information, and the means of so doing, to legitimately protect the interests of the bank and its shareholders and customers, for example, and is an issue which involves public

policy where a balance needs to be struck between the legitimate collection and use of information and privacy considerations.

The Government Task Force Draft Code of Practice seeks, on the one hand, to confirm relevant public policy issues here by the provisions noted above in Clause 15.6 of the Code, and addresses the counter balancing issue of the legitimate collection and use of information by Clause 15.7 of the Code, which provides as follows:

> Information shall be collected only for the purpose of establishing and maintaining relationships with customers, *including the protection of the institutions and customers interests.* The customer information collected for these purposes shall not be used for other purposes without the specific consent of the customer.

The Draft Code also provides (in clause 15.14) that:

> Institutions shall take such steps as are reasonable in the circumstances to protect personal information against loss and against unauthorised access, use, modification or disclosure.

The banks' position

The banking industry accepts the general propositions outlined in the Government Task Force Draft Code of Practice, but believes that greater drafting clarity has been achieved in the revisions provided to the Government Task Force by the draft Code of Banking Practice (incorporating amendments proposed by the ABA) publicly released on the 12 August 1993 by the banks.

In so far as the issues are relevant to today's discussions, the revised Code repeats many of the provisions of the Government Task Force Code outlined above and succinctly stipulates the legal position in Clause 12.3:

> A bank shall not collect information relating to customers by unlawful means.

In so far as a banker's duty of confidentiality (in relation to information collected about a customer) the general Common Law position is apposite and is encapsulated in the revised Code of Practice in Clause 12.1, which provides as follows:

> A Bank acknowledges that, in addition to a Bank's duties under legislation, it has a general duty of confidentiality towards a customer except in the following circumstances:
>
> i) Where disclosure is compelled by law;

ii) Where there is a duty to the public to disclose;

iii) Where the interest of the Bank require disclosure; or

iv) Where disclosure is made with the express or implied consent of the customer.

This reflects a classic Common Law position set out in *Tournier v National Provincial and Union Bank of England* (1924) lKB461, which remains the unchallenged authority on the subject.

Adequacy of controls

The Common Law, general *Privacy Act* provisions, and the provisions outlined from the Government Task Force Draft Code and the revised Draft Code of Practice, when operative, appropriately, in our view, implement the important issues and views set out in the ICAC report.

The banks believe that voluntary codes of practice, in this area, will ensure compliance with accepted principles without the need for legislative intervention and represent an appropriate response to community concerns. The safeguarding of confidential information is at law a paramount duty of the banking industry. The use of personal information about customers is, it is suggested, now adequately covered by the provisions referred to above.

Information confidentiality

The subject, however, of what information (including Government information) should be treated and remain as confidential is a vexed one. Alan Cullen, the Executive Director of the Australian Bankers' Association, pointed out at the "Just Trade?" ICAC Seminar in Sydney on Monday 12 October 1992 (reported at page 38 of the proceedings of the seminar) that:

> While there has been a trend to extend the scope of privacy protections in a number of areas there has been an opposing trend in relation to personal identity. The broadest manifestations of this, the Australian Card concept, failed but while that failed the *Cash Transactions Report Act* and the Tax File Number had a consequence almost as wide. Under the *Cash Transactions Act* it is an offence to conduct a bank account in a name other than that by which one is commonly known. A bank account can only be opened if a person is identified by the process contained in the Act.
>
> Vital to identification is *information* which is only verifiable from Government files and documents. Intrinsic to the identification is address. The policy objective is to prevent crime and evasion of tax but it points to

> a broader principle, that is, those who deal with others in our society have a right to some assurance about the identity of the person with whom they are dealing, including their address, and an expectation of continuity in these things while the relationship continues.

A balance must be struck

These comments indicate that there should be a public policy recognition of the legitimate use of personal confidential information. It is the extent of the availability and use of Government information, for legitimate purposes, that now needs to be determined.

The above comments raise the question whether the general rule should be that name and address data stored in Government records should be universally accessible to the public although such data is personal information and often confidential to the individual concerned.

The ICAC report concluded that the rule relating to government held addresses should either be that they are all held as confidential and protected, or that they are all publicly available, irrespective of the department or agency by which they are held, the purpose for which they are required or the person by whom they are sought. The *Privacy Amendment Act*, however, already recognises that where a person has given consent then there may be access to, or use of, certain credit information the privacy of which would otherwise be protected.

Legitimate need for information and consent

The comments by Alan Cullen at the ICAC Seminar last year that

> protected name and address data should be the exception rather than the rule, at least for the commonly used identifiers such as Government departments with widespread client bases, essential services such as water, gas, electricity and telephone, registration of drivers and vehicles, records of residential tenancy and ownership

remain the position as we see it.

Information such as that referred to above is required by banks to conduct initial credit assessment and approval of loan facilities. The move towards harsher rules upon banks to establish servicing capacity set out in the Codes of Practice and Draft Credit Legislation also dictate that banks must have access to information to enable verification of the position of their customers prior to extending credit.

There is also a legitimate public interest in a bank having access to information for recovery of debts owing by borrowers and, provided that such information is obtained with consent or is not unlawfully obtained, then there is a legitimate public purpose underpinning the reasonableness of having that information available, i.e. the cost to all bank customers and shareholders is diminished if such information is available to assist in loss prevention.

The policy of Government in this area should extend to ensuring that information availability matches the policy objective and that rules on information privacy and confidentiality are approached on a national basis.

The banks do not believe that there is need for prescriptive legislative intervention in this area, as adequate protections already existing in legislation provide offences for the improper use or release of confidential information. It is purely a question of enforcing those provisions.

An environment of openness and integrity is essential. Government must set a balance between the legitimate need for privacy of personal information and the functioning of commercial operations and information exchange.

I believe that the developing trend will be that with informed consent documentation from customers taken at the appropriate time information should be widely available. The position should be that, like banks operating under the *Privacy Act* provisions, there should be no real reason why Government information should not be available provided that it is known that this information will be made available to third parties with a legitimate interest and there is informed consent or a legitimate need subsequently shown for the information to be made available.

Conclusions

The banking industry believes that through existing legislation, Common Law principles, and the emerging Codes of Practice that there are sufficient controls to safeguard confidential information.

The public policy position should be that a reasonable level of information should be freely available, for legitimate commercial purposes, and if such is the case then it will self destruct any illicit trade in Government information as the market for such information would no longer exist.

Banks commend the Government initiatives in the area of the administration of the *Privacy Act*, particularly the Privacy Commissioner's readiness to develop a workable Code of Conduct from what was prescriptive legislation (which required massive amendments before it could be operational) and moves to a regime where necessary information is available and the basis for that availability is underpinned by the principles of informed consent or legitimacy of need.

GOVERNMENT TASK FORCE

SECOND DRAFT

CODE OF PRACTICE

18 JUNE 1993

Clause 15.1

To the extent required or permitted by law, Institutions shall observe their duty of confidentiality with regard to Customers' or former Customers' information.

Clause 15.6

Institutions shall only collect information by lawful means and shall not use or disclose information which they know or believe may have been collected unlawfully.

Clause 15.7

Information shall be collected only for the purpose of establishing and maintaining relationships with Customers, including the protection of the Institutions and Customer's interest. *Customers' information* collected for these purposes shall not be used for other purposes without the specific consent of the Customer.

Clause 15.14

Institutions shall take such steps as are reasonable in the circumstances to protect personal information against loss and against unauthorised access, use, modification or disclosure.

provided by the Australian Bankers' Association

DRAFT ABA CODE OF PRACTICE

PRIVACY AND CONFIDENTIALITY

12 AUGUST 1993

A Bank acknowledges that, in **addition to** a Bank's duties under legislation, it has a general duty of confidentiality towards a Customer except in the following circumstances:

(i) where disclosure is compelled by law;

(ii) where there is a duty to the public to disclose;

(iii) where the interests of the **Bank require disclosure;** or

(iv) where disclosure is made with the express or implied consent of the Customer.

provided by the Australian Bankers' Association

DRAFT ABA CODE OF PRACTICE

COLLECTION OF INFORMATION

12 AUGUST 1993

Clause 12.3

A Bank shall not collect information relating to customers by unlawful means.

Clause 12.4

A Bank shall on request provide a Customer or past Customer with information as to matters of fact which is readily accessible to the Bank and which may lawfully be provided. The factual information to be provided shall be limited to the Customer's address, occupation, marital status, age, sex, Accounts with the Bank and balances and statements relating to those Accounts.

INFORMATION USE AND PROTECTION

Clause 12.9

A Bank may not collect, use or disseminate information about a Customer's:

(i) political, social or religious beliefs or affiliations;

(ii) race, ethnic origins or national origins; or

(iii) sexual preferences or practices,

except where the *Bank does so for a proper* commercial purpose."

Clause 12.10

A Bank shall take reasonable steps to protect personal information held by it relating to a Customer against loss, unauthorised access, use, modification or disclosure. A Bank shall require all staff with access to personal information concerning Customers to maintain confidentiality concerning that information.

provided by the Australian Bankers' Association

SESSION 4

Union and Community Response and the Freedom of Information Issue

CHAIR: Barrie Ffrench
Commissioner
Criminal Justice Commission

CHAIR: Ladies and gentlemen: This final session will address the problem from the point of view of the Public Service Union and members of the general public. We'll also hear from Professor Chris Gilbert, of the Centre for Commercial and property law at the Queensland University of Technology.

Information privacy, or data protection, is not about *stopping* access to government information – it's about setting up a regulatory system of control. The illegal trade in government information that we've heard so much about today is a corrupt trade, and it affects, as we have seen, many sectors of the workforce. For a perspective on how the misuse of private information can affect consumers, we will hear from Tim Dixon of the Australian Privacy Commission. Government employees in particular can become involved in this illicit trade, and so for their point of view we will then hear from Brendon Kelly of the State Public Services Federation of Queensland.

Tim Dixon has been active in the privacy movement for over six years. In 1991 he conducted an extensive study of the data matching practices of the Australian taxation and social security agencies. He is Director of the Australian Privacy Foundation, Australia's only specialist non-government organisation in this field. He is also secretary of the Australian Privacy Charter Council, an organisation formed to develop a charter of privacy principles for implementation in the public and private sectors in Australia.

Australia is experiencing a crisis of confidence in our institutions of public life. In simple terms, we just don't trust our governments any more. The explanations for the deepening cynicism about governments and their promises lie in complex, political and social developments over recent decades. But they have very definite consequences for the issues before us today.

In the modern state the relationship between the individual and the organisations of the state is increasingly mediated by information flows. It is not surprising, then, that the distrust felt towards public institutions is often most evident in debate about how governments can balance the privacy rights of individuals with the need to collect, store and use personal information to fulfil the functions of the modern state.

It is useful for us to stand back from considering the detail of specific sanctions for traders in illegally obtained information to reflect on some of the broader issues involved in this debate. I don't believe we will come up with adequate solutions to the problem of the corrupt disclosure of information without understanding the wider context of the community's privacy concerns.

Understanding the community's distrust

In addition to the broadly felt alienation from public institutions and the political process, four particular factors affecting the community's confidence in the information handlers strike me. I think most observers would agree that while some of these fears are irrational, there is some legitimacy in the community's concerns.

The first factor relates to the carelessness of practices of government agencies in handling our personal information. We regularly hear and read stories of personal information records being found in the most unusual places – on a rubbish dump, in a filing cabinet sold by the police, fallen off the back of a truck; or we read of Audit Office reports exposing the lax information handling practices of major agencies such as the Bureau of Statistics. Each individual event is a one-off occurrence but the frequency of these sorts of media stories reinforces a general community attitude that people in both the public and private sector do not exercise adequate care with their personal information records. It is not surprising that a degree of cynicism is generated in the light of the repeated assurances that our personal information is secure in the hands of government agencies. For years privacy advocates who have questioned the security of personal information have been treated with derision. But people are now finding it hard to accept the strong assurances of the security of our information given when expansions to information systems are being sought.

The second factor relates to the issues before us today: the illegal trade in government information. As Adrian Roden described it in the ICAC report last year, it amounts to our privacy being for sale. Those findings reinforced the concerns which privacy advocates had voiced for years – concerns which earnt us accusations of paranoia and fear mongering. The ICAC report sent a clear message to the community that their personal information was up for grabs. As Mr Roden asked,

> What confidence can the community have in the statements of policy and attitude by large and ostensibly responsible commercial organisations when, in their conduct, it is so difficult to see those principles reflected?[1]

The third factor explaining the declining confidence in the confidentiality of personal information held by our major pubic institutions is the community's perception that government will use that information for whatever purposes they like without safeguards. This view is created by such incidents as when the police handed over to the DSS the names and addresses of people arrested at the ADIEX arms rally in Canberra. Although the charges against each of the protesters were dropped, the DSS chased up the welfare recipients among the two hundred to seek explanations for their visit to Canberra. The Privacy Commissioner's report censured the police for the action. Such incidents can become burnt on the public consciousness.

The fourth factor is the perception of a general erosion in privacy caused by the trend towards ever greater information collection, use and disclosure. The community's anxiety about the "big brother" society has been reinforced since the days of the Australia Card campaign with the progressive expansion of information technology usage by both government and the private sector – from the Tax File Number to photo identity cards. There is a feeling that this pervasive technology is running out of control and that it may be used against consumers rather than in their interests.

No-one in the public sector can afford to shrug their shoulders and say that the community's perceptions do not matter. It's a fact of life that the community is unlikely to discriminate between the practices of different government agencies. All agencies tend to be lumped together in the public's eyes. This is unfortunate, because there are significant differences in the attitudes of government agencies towards the privacy of individuals. Some agencies have a profound and serious concern for respecting privacy rights; others have problems coming to terms with the concept of privacy at all. But when one agency gets it wrong, they all tend to get tarred with the same brush. So it is in the interests of the entire public sector

---

[1] Adrian Roden, Keynote Address to *Just Trade?* Seminar on the ICAC Report on the Unauthorised Release of Government Information, Monday, 12 October 1992, p. 6.

that we take measures to restore the community's confidence in their public institutions.

But the issues raised by the unlawful release of government information goes beyond the interests of public institutions and their relationship to individuals. They influence the entire social climate. As a nation we need openness and trust from our public institutions. A strong culture of privacy is essential to keep balance and to keep faith in our society and our government. Too often we talk about the costs of privacy; without taking into account the tremendous benefits of living in a society which places a premium on freedom.

Implications of public distrust

On the other hand, there are real costs associated with the growing distrust of governments in their use of personal information. There is the immediate result that the public becomes less co-operative in providing personal information to government. If the community's resentment of intrusive government practices deepens we will see increasing signs of informational mutiny – deliberate efforts to subvert government information. As Mr Roden commented at the ICAC Seminar on these issues last year, 'once confidentiality goes, so to does its reliability. And that is fact and not fiction.'[2] Others will drop out of society and do all they can to avoid generating any kind of data trail. Finally, there are possibilities of extreme responses borne out of frustration and anger with the loss of personal privacy. This may mean that public opposition reaches the point of civil disobedience, such as the Netherlands' 1971 census which saw the court impossibly clogged with people refusing to complete their forms. It may force an extreme political solution, such as the government being made to abandon a major system.

Inadequacies of current responses

The point is that public agencies have a self-interest in maintaining or restoring the community's confidence in the confidentiality of their personal information. Yet to this point the responses of government to revelations of the corrupt disclosure of personal information have been inadequate to restore confidence. I note five reasons why.

First, it is apparent that the political will to deal with privacy issues just doesn't seem to be there. We are accustomed to hearing people mouth concerns about privacy, but when it comes to making a decision between a privacy interest and the promise of a few extra dollars, that concerns seems to dissipate. Privacy then is seen as a cost or an unnecessary curtailment of the public sector.

---

2 *Op. cit.* p. 13.

We only need to look at the slowness of governments in establishing privacy legislation and agencies to monitor policy issues to illustrate this lack of political will. The Commonwealth *Privacy Act*, for example, was initially brought out as a measure alongside the Australia Card Bill, essentially to make it more publicly acceptable. At the state level, the New South Wales Privacy Committee, with just a handful of staff, was established as an interim measure in 1975. The Queensland Privacy Committee, staffed by just one person, was laid to rest quietly at the end of 1991. Other states have lacked even these measures.

Secondly, we have relied almost exclusively on a legal response to the privacy issue. There are serious limitations on the capacity of law to achieve the kind of change necessary to restore community confidence. Laws tend to generate a reluctant, minimal compliance from agencies. There is often a misunderstanding that the privacy issue has been dealt with and resolved if an agency is complying with the law – when the law is often an incomplete and minimal set of standards, rather than a comprehensive set of protections. But privacy is a much wider issue than just a set of principles or regulations – it is a matter of the whole relationship between consumers and the organisations of the state and of commerce. There are real dangers that with reliance on law we lose sight of the true dimensions of privacy and reduce it to a set of technicalities for lawyers and technologists to wrangle over.

A third problem with the existing responses is that often privacy and data protection laws allow for blanket exemptions at the most crucial points where privacy is invaded. The exemptions granted for purposes of protection of public revenue and enforcement of the criminal law under Information Privacy Principle 11 (e) in the Commonwealth *Privacy Act* are a case in point. As the Privacy Commissioner remarked in last year's annual report, this exception is allowing the *Privacy Act* to supply a legal foundation for privacy invasive practices such as data-matching. There is a serious danger that measures for privacy protection become a mirage; something akin to have security guards on the front doors but leaving the back doors open.

A fourth problem is the lack of sanctions available against the recipients of confidential personal information, a point strongly emphasised in the ICAC Report. In many cases, the only measures taken against the illegal traders in information were internal disciplinary procedures from organisations which had authorised spending millions of dollars on buying confidential information.

A fifth problem is that while there is a growing understanding of the need for consent in the secondary uses of personal information, the existing consent practices are often artificial. When a credit applicant has a form thrust in front of them and they are told where to sign, they are not really informed about what they are signing, nor do they have any choice about consenting if they want to have

their application accepted. This is hardly likely to convince consumers that the attitudes of the financial institutions who spend millions of dollars on illegally obtained information have changed.

Developing Privacy Culture in Public and Private Institutions

Clearly, we have a long way to go to restore the confidence of the community in the agencies collecting, using and processing information. But the task is not impossible. I think the most significant challenge is to nurture a privacy culture among the information handlers of government and the private sector.

Developing an organisational culture which respects privacy starts with information handlers taking consumers' value for their privacy seriously and treating information about their private lives with respect. Surveys across Australia and the industrialised world have shown a rising anxiety about privacy erosions in the last decade. Those concerns are justified in the light of the stunning, systematic exchange of information which has been going on in New South Wales for so long.

Australians want to know and see that organisations understand their right to control the information about their lives. They want to see public sector agencies understand that they are in a relationship of trust and responsibility for that information, particularly since the information is provided under the force of legal requirement, and not voluntarily. The corollary of the hackneyed phrase that information is power is that agencies holding personal information need to recognise that this potentially gives them significant power over the individual – and therefore requires that they act with sensitivity to the privacy of the individuals whose data they possess. This is the beginning of a genuine culture of privacy.

One current initiative to develop a privacy culture in Australia is the work being done towards the creation of an Australian Privacy Charter, a brief and clear statement of what privacy means to Australians, backed up by universal principles to ensure its protection. The Charter Council was assembled by Justice Michael Kirby, President of the New South Wales Court of Appeal, and Simon Davies, the Director-General of Privacy International. It groups together representatives of industry, finance and other media, community advocates, information technologists, academics and others to develop a concise set of privacy principles to be adopted by the public and private sector in Australia. Organisations which embrace the final Charter document and take measures to implement in their own context will be making a clear affirmation of their commitment to privacy rights. Such measures may begin to rebuild community confidence in the confidentiality of personal information held by government.

Future developments

The importance of going beyond law reform in responding to the illicit personal information trade is emphasised by the prospects for future uses of personal data. The outlook through to the first decade of the next century is a continuing, exponential growth in the collection of information by government and business. As possibilities for information collection, matching, and usage grow and costs fall, information collectors will be tempted to draw an ever longer data shadow behind each one of us.

One particular development which illustrates this trend is data profiling. Data profiling is based on creating a subset of a database on the basis of characteristics identified as being associated with a particular act, risk or practice such as drug trafficking, public health risks and fraud. The US Office of Technology Assessment describes profiling procedures as attempts 'to determine indicators of characteristics and/or behaviour pattern that are related to the occurrence of certain behaviour.'[3] The report notes that profiling is an attractive procedure for government agencies because it reduces the population of likely suspects for an agency and thus can increase the effectiveness of its compliance measures.

With this kind of technology, we don't need to think too hard to imagine how the kind of information profile generated by this procedure could be valuable to commercial institutions – a point currently being highlighted in Europe.[4] Equally, it will mean that governments will have reason to access more information held by commercial institutions. There is a significant and growing mutual interest in the exchange of data.

On a broader scale, the issues of privacy and the security of confidential information will be increasingly prominent in the years ahead. I believe privacy will be one of the major civil rights issues of the early 21st Century. In the information society, it is the issue which defines the relationships of the individual to public and private sector institutions.

Conclusion

It will take time to restore the community's confidence in public institutions which handle their personal information. It will also take an appropriately comprehensive

---

3 OTA-CIT, Electronic *Record System and Individual Privacy*, US Government Printing Office, Washington DC, p. 87.

4 Yves Poullet (Dean of the Faculty of Law, Namur, France; Director of the Centre for Computer Research and Law, Namur) 'The Commercialisation of Data Held by the Pubic Sector', *Computer Law and Security Report*, September/October 1993.

response to the corrupt disclosure of confidential information.[5] In sum, there are three major elements to that response:

1. Law reform, such as through proscribing dealing in confidential information and establishing state privacy legislation and watchdog organisations;

2. Technological safeguards, such as through maintaining an audit of access of personal records and implementing levels of security.

3. Organisational change to develop a culture of privacy, embracing both internal measures such as training and sanctions and external measures such as informing consumers of personal information practices and giving them a maximum amount of control over their personal information.

It is in developing organisational cultures which respect privacy that our response is least developed. Yet only when there is a widespread understanding of the value consumers invest in their own privacy and the legitimacy of their concern will we develop an enduring resolution of these issues. Without this understanding, legal measures too often are bogged down with technicalities or become outdated by technological developments. We need to achieve a genuine understanding that an individual's personal information is *theirs*, that public officials are vested with a significant trust in handling this information, and that unauthorised disclosure of this information is a criminal act as serious as trading in stolen goods.

A failure to respond adequately to the revelations of the illegal trade in confidential information will involve significant costs – not just to individuals, and not just to the integrity of public institutions and their data, but to the climate of our whole society and to that sense of freedom which we value so highly.

---

5 Roger Clarke, National Capital Convenor for the Australian Privacy Foundation, outlined these options in a paper presented to *Just Trade?* Seminar, pp. 62-63.

CHAIR: Thank you Tim Dixon. And now let me introduce Brendon Kelly from the State Public Services Union, who will deliver a paper on behalf of Janine Walker.

Janine Walker is well known in Queensland in many areas, most recently for her work as Director of Industrial Services in the State Public Services Federation of Queensland. She is a member of many boards and committees, including as a Director of the Australian Broadcasting Corporation and a Commissioner for the Queensland Vocational Education, Training and Employment Commission.

Whistleblowers – Where Do They Go? by Janine Walker

It is very appropriate for the Commission to invite the Union to participate in this discussion on the Unlawful Release of Government Information and we thank you for the opportunity to participate. As the Union which represents the broadest possible range of State Public Sector workers we find ourselves quite frequently required to represent members caught up in the full range of actions – investigative, disciplinary and criminal – which can arise from incidents of unlawful dealing with information which is the property of the employer.

As an organisation, we totally support the policy developments which have found expression in this Commission's legislation and particularly those amendments described as the Whistleblowers (Interim Protection) amendments. There have been numerous incidents in the past of honest and brave individuals who have sought to bring wrongdoing to the attention of the proper authorities only to be persecuted and punished by so-called "proper authorities" who at best didn't want to know or who at worst were parties to the wrongdoing.

It would be naive in the extreme to believe that the legislation referred to has waved a magic wand and set straight the path for the whistleblower. Those present who are familiar with the advanced refinements of the ancient art of persecution developed by modern complex bureaucracies would mock such a suggestion. However, your legislation has at least made it possible to deal with overt actions against individuals as a consequence of their dealings with your Commission as a "proper authority" in incidents of alleged official misconduct.

But before these brave and righteous individuals take a step down the path which may lead them to the Commission's door, they often seek the advice of the Union as to how best to blow the whistle and what protection is afforded them if they do.

Your brief for today's seminar is to look at the issues which surround unlawful release of Government information which, in our experience, occurs in a number of quite distinguishable contexts. In this paper it is our intention to share with you the Union's perspective on the issues under two headings which reflect the general categories of motivation which, in our experience, underlie most forms of unlawful dealing in information we have experienced. These are

- profit
- policy and politics.

Profit

"Information is power" is a familiar cliche and it might also be said that information is profit in the modern marketplace. Government is the largest gatherer and storer of information of all kinds in our society and so it follows, as we have seen from some celebrated instances in other States, that those with access to Government data are in a position to provide what is eagerly sought on the commercial black market. From the few cases which have come to public attention of the direct sale of Government information on individuals it is clear that some of our most respected business organisations have been willing to at least turn a blind eye to these activities by individuals and profit from their unlawful enterprise.

This unlawful trade should be treated as the criminal activity that it is and the penalties should reflect the serious threat this type of crime poses to the liberties and privacy of citizens. This is an area of criminal activity where penalties are most likely to have the desired deterrent effect. Just as other criminals may not keep their profits of crime, individuals and organisations, no matter how respectable, who use illegally obtained Government information for profit – for example to generate business through mailing lists or even to speed up the collection of monies from people who might be costly to pursue by legal means – should be penalised by the confiscation of profits.
As a Union we have no brief for any member who commits a crime, albeit at the workplace, beyond assisting, if help is sought, to point the individual in the direction of appropriate legal representation.

For the Union to advise a member who wishes to "blow the whistle" on others they believe involved in such activities for personal profit is a matter of comparative ease. The process is relatively simple and the protection mechanisms well documented. Our task in advising the potential whistleblower where they should go is far more difficult if the apparent motive for the misuse of the information falls under the second heading.

Policy and politics

Senator Graham Richardson in a recent interview described the political process as 'a marketplace of ideas'. Despite the lip service still occasionally paid to the Westminster tradition of an impartial public service serving the Government of the day without fear or favour, many public sector employees at all levels find themselves drawn into the haggling and bargaining of this marketplace.

The reality is that today's senior public servants are often overtly identified with particular political and policy positions and are employed for their ability to effectively and expertly move public administration in the directions sought by the

Government of the day. This fundamental change in the nature of the bureaucracy at senior levels has had a profound impact on the operations of Government organisations.

It is significant in the context of today's subject to focus on the changes that we perceive to have occurred in the way policy advice is developed in the bureaucracy. It is our contention that the insertion of political perspective by public servants into the important formative stages of policy processes has led to situations where some public servants have judged that they cannot debate policy within the bureaucracy but must move outside it to put their views.

It is our experience that in some agencies there is a "company line" on important policy issues generated by a small group of senior officials and ministerial advisers. Officers who express a conflicting point of view are regarded as threatening and are frequently marginalised or excluded from circles of influence and from the organisation itself eventually. In such an environment, officers who hold strong views on an issue contrary to the prevailing wisdom can find themselves in a difficult dilemma. Our Union has dealt with a number of such cases where an officer, consistently denied the opportunity to argue against what she or he considers bad policy, decides to shift the policy debate to a different forum by means of conveying information to persons outside the organisation – the practice known as "leaking".

Whilst not condoning such conduct, it is hard not to be cynical when listening to the righteous anger of politicians who find themselves on the receiving end of leaks. The strategic placement of the well aimed leak is part of the stock in trade of every politician in the country. The application of sanctions to Ministerial office holders who leak Government information would soon satisfy those who think we have too many politicians in this country.

Leaking information to any person – be it the media, a politician or an interest group – is in contravention of the Code of Conduct for Public Officials and is undeniably misconduct which is quite properly subject to appropriate disciplinary procedures. My Union fully supports that position and when advice is sought from us, as it often is, by officers contemplating such an action, they are told that they cannot expect anything but the full force of legislative sanctions if they engage in such activity.

It must be said, however, that organisations who find themselves regularly subjected to the unauthorised release of policy information by disgruntled employees should look to their own processes to understand why it is happening.

Is debate at the appropriate levels part of the structured policy making process within the organisation?

Is a vigorous and rigorous analysis of policy options at the appropriate levels encouraged?

Are officers who argue an alternative position valued for their contribution even if their views are not reflected in the final outcome?

Is the organisation visibly capable of distinguishing between the permanent "knocker" and the properly motivated dissenter?

Whilst investigating leaks and taking action against offenders when they are identified is a quite proper response, organisations should also examine their own management of the relevant issues.

Conclusion

In conclusion, it is worth returning to a fact which was briefly mentioned at the outset, that is that Government is the biggest gatherer and scorer of information in our society. Further, there is no area of human endeavour which is not touched and influenced by Government policy at some level. With such givens, it has to be appreciated that the imposition of security measures and the prosecution of offenders will never be measures sufficient in themselves to protect Government information. At the end of the day, the security of Government information is dependant on the ethical behaviour of public sector workers.

It is difficult to successfully communicate the importance to society of an ethical public service, if, at the same time, there is a consistent message that working in the public sector workers are, by definition, lazy people who just rip off the system at every opportunity. I would take this opportunity to stress the obvious correlation between the morale of the public service and its receptiveness to strategies aimed at lifting commitment to ethical work standards.

CHAIR: Thank you Brendon Kelly.

Our last speaker today is Professor Chris Gilbert.

Professor Chris Gilbert, a Solicitor of the Supreme Court of Queensland and a Barrister and Solicitor of the Supreme Court of the ACT, is currently Clayton Utz Professor of Law at the Queensland University of Technology. He has been an academic since 1970, and has published widely in the areas of Constitutional Law, Contract Law, International Trade Law and Intellectual Property Law. He was a foundation member of the Fraser Government's Human Rights Commission from 1981-1984, and he has wide administrative experience.

Introduction

Professor Finn has said that the constitutional landscape in Australia with respect to public pressure for freedom of information legislation is divided into three phases: first, there was the 'public interest paternalism' phase. Deference to the Crown, cloaked in the language of 'public interest', resulted in the government being left to decide what and when official information should be made publicly available. The second phase, 'governmental authoritarianism', allowed governments to equate their interests with the concept of the "public interest", allowing governments to elevate their interests over all others. This included the coercing of subservience from its officials through stringent secrecy regimes. The third phase, and the most recent one, is the 'liberal democratic' phase. It is the current one and is marked by things such as freedom of information and privacy legislation and the now less deferential attitude taken to government to privilege cases: P Finn, quoted in *Eccleston v. Department of Family Services and Aboriginal and Islander Affairs* (Decision S 15 of the Queensland Information Commissioner, 30 June 1993) p.11.

Finn further comments that contemporary Australian law is in a period of transition from the second to the third of these phases: *Eccleston*, above, p. 11. The reason behind this change in the legal approach to government-held information is well summed up by McHugh J.A. in *Attorney General (U.K.) v. Heinemann Publishers Pty Ltd* (1987) 10 N.S.W.L.R. 86, p. 191:

> ... but governments act, or at all events are constitutionally required to act, in the public interest. Information is held, received and imparted by governments, their departments and agencies to further the public interest.

On the general question of when will the general law protect from public disclosure confidential information in the possession of governments, the following statement of the law by Mr Justice Mason of the Australian High Court is instructive:

> The question then, when the Executive Government seeks the protection given by Equity, is: what detriment does it need to show?
>
> The equitable principle has been fashioned to protect the personal, private and proprietary interests of the citizen, not to protect the very different interests of the Executive Government. It acts, or is supposed to act, not according to standards of private interest but in the public interest. This is not to say that Equity will not protect information in the hands of the government, but it is to say that when Equity protects government information it will look at the matter through different spectacles.

> It may be a sufficient detriment to the citizen that disclosure of the information relating to his affairs will expose his actions to public discussion and criticism. But it can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticise government action.
>
> Accordingly, the court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.
>
> ... if ... it appears that disclosure will be inimical to the public interest because national security, relations with foreign countries or the ordinary business of government will be prejudiced, disclosure will be restrained: *The Commonwealth v. John Fairfax & Sons Ltd* (1981) 55 ALJR 45, p. 49.

In other words, as Dean comments, the onus of proof as to the obligation of confidentiality in respect of government-held information is effectively reversed. Unless the contrary is shown by the government, the public interest is in open government and in the disclosure of government information: R. Dean, *The Law of Trade Secrets* (Law Book Co., 1990), p. 173.

The general law's predisposition towards open access to government-held information is now broadly reflected (with major exceptions) in the *Freedom of Information Act* 1991 (Qld.). Section 21 of the Act gives a person a legally enforceable right of access (subject to the Act) to documents held by government agencies and Ministers. Furthermore, in s. 5(1) of the Act, the Queensland Parliament has expressly recognised that, in a free and democratic society, the public interest is served by promoting open discussion of public affairs and enhancing government accountability. Also, the section notes that the community should be kept informed of the government's operations, including the rules and practices followed by government in its dealings with the community.

The general point to be gathered from this is that the philosophy of openness and accountability that underlies the *Freedom of Information Act* reflects modern principles of the general law, rather than running counter to it.

The Freedom of Information Act and Government Confidentiality

Despite the general philosophy of access to government information that underlies the *Freedom of Information Act*, the Act of course, recognises that there are many situations where information held by government should not be released. Sections 36-50 of the Act list 15 situations in which, to a greater or lesser extent, government

information may lawfully be withheld from public disclosure. These 15 categories will be well known to most of you, and I need not list them here in detail. It is sufficient to draw attention to four of them which are probably the most relevant to today's conference: matters affecting personal affairs (s. 44); matters relating to trade secrets, business affairs and research (s. 45); matters communicated to the government in confidence (s. 46); and matters covered by secrecy provisions in enactments (s. 48).

The provisions of s. 48 are of particular relevance to the subject matter of this conference. Various Queensland statutes contain secrecy provisions which, in some shape or form, prohibit employees of government departments or various statutory authorities from disclosing information gained by them during their employment. To the extent that these secrecy clauses come within the language of s. 48 (and not all of them will), government information caught by those secrecy clauses need not be disclosed to the public by virtue of s. 48 of the *Freedom of Information Act.*

However, it is worth nothing that subs. (3) of s. 48 provides that the section has effect for only two years from the date of assent to the *Freedom of Information Act.* This means, in effect, that s. 48 expires after 19 August 1994. From that date onwards, it becomes highly arguable (though by no means certain) that any secrecy clauses in Queensland legislation that pre-date the *Freedom of Information Act* may well be regarded as overruled by the (later) *Freedom of Information Act.* It will be arguable that the only effective secrecy clauses will be those contained in legislation that post-dates the freedom of information legislation.

So, at least until 19 August 1994, present secrecy clauses in State enactments will usually (but not always) be an effective way of preventing the public disclosure of such government information as is covered by those clauses. Yet it should be remembered that not even the exemption categories of the *Freedom of Information Act* compel the government to withhold from the public secret or confidential information. The exemption categories in the FOI legislation permit the government to withhold information of the kind coming from within the exempt categories. These exemption categories do not compel the government to withhold that information: see the permissive, not mandatory language of s. 28(1) of the *Freedom of Information Act.* In other words, the exemptions in the FOI legislation are basically discretionary in nature. This much becomes clear when one reads s. 28(1) of the Act in conjunction with s. 14 of the Act. This latter provision states that, amongst other things, the FOI Act is not intended to prevent or discourage other ways of giving access to government-held information, if this can properly be done. In other words, I think the correct way to read ss. 36-50 of the Act is not as if they were a mandatory code requiring non-disclosure, but merely as a permissive regime, authorising governments to withhold the relevant classes of information if the government so decides (which of course they usually will!).

A culture of reluctance to embrace FOI?

In spite of the fact that the Queensland FOI legislation gives more than ample opportunity, I would have thought, for government agencies to protect their information from public disclosure by using any one or more of the 15 exemption categories, it would seem that some government circles find even the present FOI legislation dangerously radical and subversive. The following quotation from the Queensland Information Commissioner is sad but instructive:

> Already, after less than a year of operation of the FOI Act, views have been publicly expressed by some Ministers and administrators that the FOI Act and other Fitzgerald inspired accountability mechanisms have "gone too far" and constitute an expensive and inefficient distraction to the performance of the main task of government. One can anticipate a lack of sympathy in many quarters of the Queensland public sector to the inconvenience posed by the added and time-consuming burdens of new accountability measures and demands for greater public scrutiny and public participation, particularly at a time when the Queensland public sector, in common with other Australian governments, has been embracing the ethic of the "new managerialism", designed to engender and exploit a corporate management public service mentality in the interests of cost cutting and obtaining the government's desired outcome with the most efficient use of limited public resources: The *Eccleston* case, above, p. 26.

This may also explain a worrying trend that I have noticed in my own private practice. There is a small but significant trickle of government agencies and statutory authorities asking how they can secure a specific exemption (specific, that is, to their own organisation) from the *Freedom of Information Act*. They basically want to see themselves added to the list of exempt government and government-related bodies contained in s. 11(1) of the FOI Act. In most (but not all) cases, the advice is simple: procure a Regulation specifically exempting your organisation from the FOI Act, pursuant to the regulation-making power in s. 11(1)(q) of the FOI Act. It seems that this latter provision was not recommended by the Electoral and Administrative Review Commission who drew up and recommended the original FOI Bill. Indeed, if my memory serves me right, EARC specifically recommended in its FOI Report against including in the FOI legislation a power to exempt bodies from the Act by way of regulation.

It would appear that there are some people in the ranks of the Public Service and the statutory authorities who have a less than complete sympathy with the Queensland Information Commissioner's thought that '(a) certain amount of inefficiency in getting things done should be a burden that democratic governments are prepared to accept as the price of honouring the higher values of the democratic process': the *Eccleston* case, above, p. 26. Perhaps this is not entirely surprising given that "inefficiency" and "democracy" are not normally noted as being the hallmarks of the "new managerialism".

Conclusion

Over the last few years, the general law has been moving away from total adherence to the view that governments have an automatic right to keep their information secret and confidential. Instead, the general law is increasingly recognising that governments hold their information in trust for the general public. Withholding this information from the public gaze may be justified, according to the general law, only if the public interest is thereby helped. Increasingly, the general law is recognising that, so far as government-held information is concerned, the public interest will, more often than not, be satisfied by disclosing such information, not concealing it. The *Freedom of Information Act* 1991 (Qld) is a recognition and an adoption by the Queensland Parliament of these trends. Yet, the Act tries to counter-balance this trend towards freedom of access by protecting at least some categories of information that the Parliament has judged to be deserving of confidentiality and secrecy in the hands of government. Yet, anecdotal evidence and public comments to a like effect by the Queensland Information Commissioner indicate, sadly, that the FOI legislation may be too much of a reform for some government agencies and statutory authorities. Education towards access and openness, after decades of secrecy, is apparently going to take much longer to change this aspect of the bureaucratic culture. It also seems that the "new managerialism" which afflicts most of the public sector feels itself thwarted by mechanisms of access and accountability.

Yet, perhaps more than ever before in modern Australian history, some form of public access and public accountability by governments is increasingly necessary. Apart from the over-worked (but totally accurate) aphorism that an informed public makes for a better-working democracy, the slow but inevitable death of the concept of a neutral and apolitical public service also requires, I would suggest, mechanisms ensuring public access and accountability. Increasingly, governments throughout Australia of all political persuasions no longer want neutral, apolitical professionals in the middle and upper management ranks of the public service. Governments want people of similar ideological persuasions who will sympathise with the prevailing ideology of the government of the day, and thus help make the government's policies work. Given that middle and upper management in the public service is under increased pressure to tow whatever line is set by a current government, it is important that any consequent government manipulations of the public service intended to bring about a potential party-political benefit should be capable of legislation. In the old days of a Westminster-style neutral and professional public service, public scrutiny of that public service and its information was perhaps not so necessary. Today the increasing (but always vociferously denied) politisation of public services around Australia is yet another factor that undermines any defence of a need for government confidentiality and bolster the philosophical and practical appeal of Freedom of Information laws.

QUESTION AND ANSWER SESSION

Ffrench — Thank you Chris Gilbert.

Question 1 — A question to you, Chris. Unfortunately we haven't had the opportunity to look at your paper beforehand and there's a point that I'm not quite sure about. In the first half of your paper you referred to the recent High Court decision and then talked about Cabinet documents. Are you essentially stating that sections 36 and 37 of the *Freedom of Information Act* are the only ones likely to ultimately stand a chance, or are you saying something different?

Gilbert — I wouldn't use the language that you've chosen but yes that is what I'm saying. In a very recent and sudden backwards step in that respect, the courts have recently decided that they want to put a virtual blank immunity on cabinet discussions, cabinet deliberations and submissions of cabinet against public display of the courts in litigation, and the High Court has said, and I have no doubt this will be followed as it must be by every court in the country, that, except where cabinet information and deliberations are needed to expose corruption and criminal conduct in high places in government, it is virtually inconceivable there will be any circumstances in order subordination (138) where cabinet deliberations and submissions should be publicised. So yes I think that unless in future a government is prepared to interpret very liberally the cabinet exemption provisions in section 36 what you say will come to pass. Yes, the High Court decision in *Northern Land Council* has given a great encouragement for governments to seek to withhold, rightly or wrongly, cabinet information.

Ffrench — Thank you. We do have time for two more questions if there are such. No? Well that being the case it's my pleasure now to introduce Professor Western to you. You've heard a wealth of information and opinion from this morning and you've seen three of the part-time Commissioners acting as chairpeople during these sessions. Obviously the organiser of the conference thought that the fourth one had all the brains and he was the one who was going to sum it up. Professor Western is not only a part-time Commissioner of the Criminal Justice Commission; he has been Professor of Sociology at the University of Queensland since the 1970s. He has degrees from the Universities of Melbourne and Columbia. He is a Fellow of the Academy of the Social Scientists in Australia. He is widely known and respected as a sociological consultant, has been a

lecturer with the Australian Development Assistance Bureau, a consultant to the International Association for Cultural Freedom, the International Development Program of Australian Universities in the Philippines and the Commonwealth Department of the Environment among many others. John Western.

Summary – Unlawful Release of Government Information by Professor John Western, Commissioner, Criminal Justice Commission

Thank you Mr Chairman. Well, you will presently see that a lot of what the Chairman had to say is perhaps of dubious validity. I've been handed quite an impossible task of trying to sum up what's happened in this seminar through the day, but I'll give it my best shot and see what happens. I'll try to do two things. I'll very briefly review the four sessions that we've heard and then take it a step further and say what I felt were the major things that came out of these discussions.

I don't think we've heard a great number of answers. We've heard a number of concerns and a number of questions raised and I'll try to summarise those in an obviously abbreviated form. But before I do that let me quickly go through what we've heard. It seems to me that we can categorise the four sessions in the following way. In the first session we heard what the problems are in information and privacy. We heard from Mr Temby, Barry Smith and Mr Justice Spender. Then in the second session we were confronted with sum of the controls that are available to look after the problems that were raised in the first session and we heard three papers directed to those issues. In the third session we learned about the importance of information to the private sector, and the speakers noted that the organisations they represent recognise the importance of confidentiality and the problem of balancing their need for information against the need to protect privacy. And finally, we've just had three papers which have dealt with the questions of information and privacy from the point of view of consumers.

Now what did those people all have to say? Ian Temby introduced us to the issues by saying that the unlawful release of government information is a widespread national and indeed he believes an international problem. It won't go away, but there will be some possibility of controlling the unlawful and the illegal use of government information. Humankind being what it is and human nature, if there's such a thing, being what it is, it's unlikely that we'll ever be able to rid ourselves completely of illegality in this area, but we can exercise considerable control. Barry Smith echoed that view, arguing that since the information society which we now have depends very heavily on technology the problem of the unlawful release of information is likely to be with us for a long time. The emergence of large scale databases makes it more possible for data to be used illegally. Justice Spender talked about the fine line dividing the public's right to know and appropriate secrecy provision. He argued that we need a principled and a consistent regime regarding the government's release of information. The conditions under which information can be released have to be clearly stipulated and spelt out. He also stressed the fine line between the release of information and the people's right to privacy. Those three papers identified the problems and set the scene for what was to come.

The three papers in session two dealt with policies developed for maintaining the secrecy of information. Jim Hann talked about the use and management of information in the Queensland Police Service. He told us that the policies regarding the release of information by the QPS are consistent with ICAC guidelines. He outlined the conditions under which criminal histories are released and the protection that's provided to the person on whom information is being sought. He also described the conditions under which information is released to the media and information security arrangements that are put in place by QPS for computer access. Nicholas Chantler took a different tack. He talked about the importance of information security, but he also pointed out the manner in which both public and private sector agencies are perhaps lax in ensuring security of information, particularly computer information. He described how sensitive information can get into wrong hands. He described to us how hackers get their information and what sort of information gets into computer systems underground. He also described how information escapes – how it escapes in deliberate ways and how it escapes in inadvertent ways. And he painted an interesting picture for us. Kevin O'Connor from the Privacy Commission talked about corrupt disclosure and the role of information privacy principles. He gave us an introduction to the *Privacy Act*. He talked about agencies being encouraged to adopt security provisions. He described the activities of the Privacy Commission. He suggested that agencies should be encouraged only to use data for the purpose for which it was collected. Sometimes this is not adhered to, sometimes the purpose for which the data are collected is not clearly defined. He discussed his Commission's involvement in the ICAC inquiry and identified a significant issue as being one of insider abuse, highlighting the need for agencies to put security provisions in place. And that ended the discussion on the control aspects of release of information.

Then we had the private enterprise response. We heard first from Graham Jones of the Insurance Council of Australia. While noting the importance of information to the private sector, he stressed the importance of information being obtained through legitimate channels. He argued that information was necessary to contain the cost of fraud, which is a major concern of the insurance industry. He also suggested that a balance is needed between the need for information to control fraud and the demand for privacy provisions. Chris Bishop, Director of the Australian Bankers' Association talked about bankers and confidentiality, also seeking a balance between confidentiality and access to information. He stressed the importance of ensuring that individuals provide informed consent before information about them is released. He argued that banks already provide sufficient controls to protect privacy through their codes of privacy and confidentiality.

We then moved on to this final session where we heard from consumer representatives. Tim Dixon talked to us eloquently about restoring community confidence in confidentiality. He argued that a culture of privacy is essential. A culture of privacy which spans society I suspect. The right to privacy he said is an

essential right, one likely to be a key civil rights issue in the next couple of decades. He said there was widespread consumer suspicion about information available about them in the public sector. He said the reasons for this suspicion were often justified. It was a general social concern. He also pointed out however that an understanding of the importance of privacy by private sector agencies was developing. He also pointed to the fact that it's a matter of balance between the release of information and privacy. He expressed however a concern about a lack of political will to do anything about legislative provisions to ensure privacy. If informed consent is to be a requirement then it has to be a real rather than apparent informed consent. Privacy he said was going to be a central issue in the information society in which we're already living but which we'll be living perhaps in a more pronounced way in the decades ahead. Brendon Kelly gave us a union perspective. He talked about the importance of whistleblower legislation. He talked about the concern about private sector connivance in breaches of confidentiality. He talked about the fact that the union movement is discouraging in an active way union members from acting illegally in leaking information. He talked about the importance of ethical behaviour among public sector workers. Finally, Chris Gilbert talked to us about government confidentiality and freedom of information. He addressed a particularly significant problem, that being the confidentiality that the individual likes to feel he has as opposed to his right to know about the rest of the community. The problem is to achieve some sort of a balance between the individual's proper concern about their own privacy and the society's concern about freedom of information and the right to know. These of course have to do with aggregates of individuals rather than the single individual. He talked briefly about the history of what is or what should be confidential and how this has changed over time. He suggested that at the present time there are in fact very few categories of government information that cannot be disclosed, cabinet debates being one such body of information. Public interest requires government affairs to be open and examination of the Queensland *Freedom of Information Act*, and a discussion of what is available through public access and what is not, formed the basis of the latter part of his talk. He noted the desire by more and more public sector agencies to gain exemption from the Act. Finally he made what I thought was a very important point. He said public access is important because governments no longer want dispassionate higher level management, dispassionate higher level bureaucrats and public servants. There is pressure on management, high level government public servants to tow the party line, to tow the government line. Where independence of the public service is lacking then public access to information perhaps becomes even more important.

Well that's a brief summary from the perspective of one person as to what was going on. What can we draw out of all that? Let me just make a few comments. I think there are larger questions that need to be considered, many of which, of course, were raised today. We need to ponder if too much information held by government agencies is deemed to be confidential. We need to assess the criteria by which information should be held confidential because surely regard must be given to the

nature of the information being held and the basis upon which it was obtained. Was it volunteered or was it demanded? For what purpose is such information being sought? We need to ask if the rules for what can and cannot be released are clear and clearly understood and assess whether there is fair and equal access to information that can be legally obtained. Is sensible uniformity and consistency about the release of information enforced? Should information given by private individuals to a government agency, because they are required to do so, be made available for commercial purposes? To what degree is sensitive and confidential information protected from those with a corrupted intent? And to what extent do agencies seek to guard this information from unlawful release? Examples ranged from commercially sensitive information on specifications, contracts or tenders that would provide unfair commercial advantage, to access by prospective employers to police records and medical data including data on infectious diseases.

Ian Temby said that the problems revealed by ICAC's report are not limited to New South Wales. If this is true, then I hope that today's proceedings will put the illicit traffic in information on the corruption prevention agenda in Queensland. If this happens, then the CJC will have done its job by promoting this debate. Thank you for attending and for being an attentive, patient audience and for raising important questions for discussion. On your behalf I thank my colleagues who chaired the various sessions and finally and most importantly, our thanks to the various speakers who have generously given of their time and experience in assisting all of us to come to terms with some of the issues involved in the unlawful release of information. Thank you.

CHAIR: Those who occupied the grave yard shift after afternoon tea know what a myth it is to keep an audience of interest. I'd like to thank the four speakers very much indeed. I'd like to thank the Royal Institute of Public Administration and the Corruption Prevention Division of the CJC who organised this conference. I'd particularly like to thank you who have stayed, who've listened. Your influence on attitudes and practices will determine how successful this conference has been. Thank you very much.

APPENDIX 1

The ICAC Report and One Year On by The Honourable Adrian Roden QC, Nikko Hotel, Sydney, 24 June 1993

Introduction

It is difficult to pick up a newspaper in Sydney these days without the letters ICAC somewhere in a headline. It may be a report of a public hearing. It may be an attack on the Commission by a politician. It may be editorial or other journalistic comment on the Commission's performance, or speculation about its future.

In many respects the Commission these days suffers from too high a profile.

For a body like the ICAC, publicity should be valuable. It is essential to its role as an exposer of corrupt conduct. And it would be difficult for the Commission to perform another of its valuable roles, that of public educator, without it.

But the high profile the ICAC has today, it has mostly for the wrong reasons.

Whether by popular demand or by media decree, the emphasis is generally on the Commission's interplay with politicians, and the perceived impact of its decisions on their fortunes and its own future.

That necessarily distracts attention from the Commission's main purpose and function.

Then there are those who criticise it for not acting like a court. Of course, it does not act like a court. It isn't a court, and it would be wrong for it to act as if it were. And there are those who criticise it if its investigations do not lead to a host of prosecutions. That also is not its principal purpose. It is not there to prepare cases for prosecution. It is not intended to be a super police force. Criticism of that type is sometimes based on a misunderstanding of the true nature and purpose of the Commission. Sometimes, perhaps, it is more calculated and mischievous.

The investigation into the unauthorised release of government information was thankfully free from political distraction, and provided the ICAC with an opportunity not only to perform one of the very important functions for which it was designed, but also to be seen to be doing so. The Commission was able to exercise its investigative powers and expose significant and widespread corrupt conduct which had become entrenched in parts of the public sector, and which violated the rights of individual citizens. It was able not only to expose the corrupt conduct but also to recommend means by which its occurrence in the future might be kept to a minimum. The Commission was able to do that, in circumstances in which the conventional police and court system could not.

One of the valuable lessons to be learned from this investigation, I believe, is that a body such as the ICAC is necessary, if results of that type are to be achieved. Those results were only achieved in this investigation, and were only achievable by the use of the Commission's special powers. By that, I don't mean telephone taps or secret surveillance. There was none of that. There were no cloaks and no daggers. I mean the simple power to require that people answer questions, and that they answer them truthfully. The proper exercise of that power, combined with the use of search warrants obtained from magistrates and other normal investigative techniques, produced a great number of admissions. Those admissions and the other evidence enabled unchallenged findings to be made, not only about the conduct of individuals, but also about defects in management and systems, and a serious want of integrity which spread from sections of the public sector into private commercial and financial institutions, in some instances at a very high level.

Finding facts when significant corrupt conduct has occurred, exposing and explaining that conduct. and proposing means whereby it may be avoided or at least minimised in the future that is the true purpose of the ICAC.

That is what it was able to do in its investigation into the unauthorised release of government information. It did not observe all the niceties and fox-hunting rules of court procedure. Nor was it subject to all the restrictions under which police investigations labour. The Commission simply did the job for which it was designed and created.

The success of the Commission's work, in this as in all its investigations, depends upon the extent of what it exposes, and the value of what it proposes. Its work is largely wasted if its proposals, or recommendations, are ignored. Nobody expects them to be adopted and acted upon in every case. But at least they can be considered: where necessary they should be debated, and where appropriate they should be implemented.

That makes the 'And One Year On' part of the subject of this address important.

As I said in the outline which was distributed yesterday, conferences like this provide opportunities from time to time to draw attention to outstanding recommendations, and to monitor progress with regard to them.

What the investigation revealed is a massive trade involving:

- invasion of privacy;
- breach of public trust by public officials, and
- corrupt conduct both by public officials and by those who dealt with them.

The extent of that illicit activity is reflected in the fact that the ICAC Report contains some 273 findings of fact, and names 155 persons as having engaged in corrupt conduct and a further 101 as having engaged in conduct causing, assisting or encouraging corrupt conduct. None of those findings has been the subject of challenge through the courts or elsewhere. What little comment there has been by persons adversely named, has been an attempt to justify their conduct on an end-justifies-the-means basis.

An appreciation of the amounts of money generated by the illicit trade can be gleaned from the fact that on the basis of disclosures made to the Commission, assessments of income tax and penalties in excess of $2 million were raised, and $712,000 of that sum had been recovered before publication of the Report. Those assessed are a small percentage only of the people involved in the trade, and their earnings a small percentage only of the total sum derived from it.

In this Address I propose to examine the investigation and its consequences by considering

- the principal findings;
- the implications of those findings;
- the recommendations made, and
- action subsequently taken.

The principal findings

The 273 findings of fact are made, and the evidence on which they are based is analysed, in the detailed Part of the Report in Volumes II and III. For those for whom 1250-odd pages are intimidating, those findings are collated and appear as a summary in Volume I commencing at page 55. For present purposes it is sufficient to quote by way of illustration the first four facts as summarised there. As I do so I omit the names, which of course do appear in the Report

1. Over a period from about 1982 to 1989, (a private inquiry agent) corruptly purchased confidential government information from Senior Constable (X) a serving, police officer. It included information from DMT RTA records criminal histories and other police records.

2. Constable (X) released the Information he corruptly sold to (the private inquiry agent) without authority and in breach of his duty as a police officer.

3. In the course of obtaining that information, Constable (X) from time to time used the registered numbers and personal access codes of other police officers to gain unauthorised access to the police computer system.

4. Constable (X), without authority, also gave (the private inquiry) information relating to police methods of storing and releasing both manual and by computer. (The private inquiry agent) used that information to obtain criminal history information by telephone falsely representing himself to be a police officer when so doing.

When that senior constable became unavailable to him through a breakdown in their relationship in 1989 the private inquiry agent found another paid source, this time a serving detective sergeant of police.

In all, 37 of the public officials found to have improperly released were serving police officers at the time, ranging in rank from Constable to Chief Superintendent. Eighteen of them were still in the Police Service when their evidence was taken. Another principal

source was the Roads and Traffic Authority. There were 18 officers of that authority and its predecessor the Department of Motor Transport found to be involved in the improper release of from department records. Fourteen of them were still employed in the RTA when their evidence was taken.

Other departments and agencies from which information was improperly released include the Sydney and Prospect County Councils and a number of Commonwealth bodies – the Department of Social Security, Telecom, Medicare, the Department of Immigration and the Australian Taxation Office.

A lucrative business

For the officers who sold the information, it was a very lucrative business. For some of them, the illicit sale of information was their principal source of income. The following figures all come from admissions made to the Commission:

- Particulars of the electricity consumers in a single building in Sydney sold by an officer of Sydney Electricity to a private investigator for $1000.

- RTA official received over $100,000 from sales of information to three of the several private investigators with whom he dealt.

- Another in the same department who had been selling information for more than ten years admitted earning $18,000 from the trade in his last operations.

- Yet another RTA official received more than $2,000 a month from his sales of information to one private investigator.

- A Detective Senior Sergeant of Police who was officer in charge of at a large Sydney suburban Police Station earned up to $560 from a single hour-and-a-half sitting at a police computer terminal. He operated for a number of years, and received and answered requests by facsimile, using a machine given to him for the purpose by a private inquiry agent client. When his business was at its peak, he made over 300 unauthorised computer accesses in a three day period.

Private Investigators

Most of the information was purchased by private investigators. It was the principal business of many of them. Their sources were corrupt public officials. Their customers included leading banks, finance and insurance companies and solicitors some of whom openly advertised their wares. For private investigators, this was a multi-million dollar industry. As with public officials, admissions enable some specific figures to be given.

- One private investigator estimated his outlay on social security purchased from within the department, at between $40,000 and $50,000 a year.

- Another private investigator estimated his income from the sale of over a two year period at $100,000.

- Invoices issued by another private investigator to a bank for 'inquiry services over 18 months' totalled $186,000.

A list of purchasers, without whose support the illicit trade could not have prospered as it did, reads like a Who's Who of banking and other financial institutions. The list Includes Westpac, ANZ, NAB and the Commonwealth and Advance Banks, New Zealand Insurance, Manufacturers' Mutual, the Government Insurance Office and NRMA Insurance Limited, and Custom Credit and Esanda Finance Corporations.

Sale is not the only means by which the information was improperly released.

Some of the information was released by public officials without payment, generally on an "old mates basis" to former colleagues employed in other departments or in private industry, or working as private investigators. Some was exchanged under an informal arrangement involving officers of a number of State and Commonwealth departments and agencies and some commercial institutions.

Confidentiality of information released through the Club was not always respected. One bizarre consequence was that a number of estate agents had access to Department of Social Security information through officers of Prospect County Council.

Persons employed by banks and other private institutions gained admission to the Club, by trading information about their employers' customers. One person who had formerly been employed by a finance company retained her Club membership and used it to obtain Telecom and social security information which she sold to private investigators. In turn it was re-sold to banks and others.

Matters referred to this point illustrate findings relating to individuals. There were of course many more such and together they established that confidential government information had been freely available through a vast illicit trade. That conduct and that trade were in turn made possible by defects in systems and laxity in management. The Commission made a number of findings with regard to those matters also.

Three illustrations can be given:

- The Commission was interested to know the official policy regarding the confidential Information. A number of government departments and agencies were asked. The policy statements received showed a striking lack of consistency. It became clear from the evidence that a number of public officials did not know what they could properly disclose, or to whom or in what circumstances they could properly disclose it.

- From time to time and under changing rules made by the Department or Authority itself, motor vehicle registration and driving licence particulars have been publicly available, or available to those with a genuine interest. Yet because of bureaucratic delays, insurers, lawyers and others entitled to the information have frequently preferred to buy it on the illicit market from private investigators.

- The police computer system was protected by restricted access and the use of individual passwords or access codes. Yet a number of corrupt officers were able to access the system in the name of others by getting to know their passwords and using them without authority.

Implications of the findings of fact

Commissions like the ICAC are not concerned solely, or primarily, with identifying offenders and enabling prosecutions. Their principal goals are:

- to expose corrupt conduct – in the case of the ICAC, corrupt conduct in the public sector;

- to draw attention to the circumstances which enabled that corrupt conduct to occur; and

- to point to means by which it may be deterred, discouraged or minimised in the future.

That had to be done in this Report.

From the three facts relating to systems and management to which I have just referred, the Commission identified and reported the following circumstances as having contributed to the context in which the corrupt conduct had prospered.

- There had not been any consistent policy to determine what information should, and what information should not, be available to the public.

- Access to information that had been publicly available had frequently been associated with such delay that a parallel illicit trade had developed, with greater speed its prime selling point.

- Information that had been held as confidential had generally not been well protected. Rudimentary precautions had not been taken with the systems that had been in place.

Those, and other circumstances to which the Commission drew attention, were the basis of a number of recommendations which were made in the Report and to which I shall shortly refer.

Inadequacies in the law

The other circumstances identified as conducive to the corrupt conduct arise from what were seen as inadequacies in the law. They relate to:

- data protection, and in particular the criminal sanctions for improper release of government-held information;

- the offence of bribery;

- regulation of the private investigation industry; and
- the criminal liability of corporations.

The law relating to data protection was found to be wanting in many respects. Necessary criminal sanctions were lacking.

A perfect illustration is the failure of a prosecution of a private investigator who had openly advertised for sale information from a variety of government departments including the Department of Social Security. The investigator bought and sold the "confidential" government information, and created and maintained his own database containing personal particulars of up to 10,000 people at any time.

As the ICAC report records the magistrate who dismissed the charges, said:

> The evidence discloses that (the private investigator) had that information in his possession there is no dispute about that, and in fact the defence concedes that... The information he had was the names and addresses of social security beneficiaries including the type of benefit they were receiving and the last date on which it was paid.

Yet it could not be shown that he had contravened the particular provision of the law artificially chosen as the basis of the prosecution. Neither possessing nor selling the information could be charged as an offence.

That matter was prosecuted under Commonwealth law. The position in New South Wales is no different.

Bribery

Uncertainties and inconsistencies in the New South Wales law relating to bribery and official corruption had been referred to in earlier ICAC Reports, principally the Report on North Coast Land Development. Express recommendations for reform of that law were made in that Report and referred to and repeated in later Commission Reports. When the Report on the Unauthorised Release of Government Information was published in August 1992, more than two years had passed, but the law remained the same. There were no proposals for change before the Parliament, and the matter had not been debated. In more than two years there had been neither action on the recommendations nor rejection of them.

The private investigation industry

Consideration had been given to the position of commercial agents and private inquiry agents prior to the Commission investigation.

A report commissioned by the Business Deregulation Unit of the Department of Business and Consumer Affairs in 1990 recommended repeal of the relevant legislation and that the industry be left in effect to regulate itself. Mr. R J Bartley, who produced the report, was impressed by the Institute of Mercantile Agents and the National Association of Investigators.

The ICAC Report, with the benefit of facts disclosed by its investigation, took a vastly different position and called for stricter regulation.

The Report records that a number of members of the Institute of Mercantile Agents, including past and present office holders, gave evidence and admitted a heavy involvement in the illicit trade in government information. The ICAC was told that sources were openly discussed at their meetings. Members of both associations admitted lying on oath to the Commission. The President of the National Association of Investigators admitted purchasing DMT/RTA and criminal history information from a serving police officer. He sold both types of information to the Government Insurance Office – over 250 traffic checks and 85 criminal histories of which the Commission is aware, charging for them at $12 and $50 each respectively. On one invoice he charged and was paid $7,700 for those 'discreet inquiries'. He told the Commission that the greater part of that money was paid to the police officer for improperly releasing the information to him. Counsel assisting the Commission described his transactions with the Government Insurance Office and the police officer as Government - funded corruption.

The criminal law relating to corporations

The major financial institutions that contributed so greatly to the illicit trade generally asserted that the purchases of improperly released government information made in their names were contrary to corporate policy. Responsibility, they said, rested with individual officers below senior management level. That did not always accord with the facts. The ICAC Report records that in some instances there were what are described as transparently unjustified attempts to limit responsibility to lower ranks than those among whom the practice had not only been approved, but actively engaged in.

Under the present law it is difficult, if not impossible, to make corporations criminally liable, without establishing participation or at least knowledge within or very close *to* the boardroom. The *Tesco* principle seems to have that effect.

In the Report the Commission argues that the principles of criminal liability presently applied to corporations can have the effect of fostering, rather than deterring, corrupt and other forms of criminal conduct.

Defective systems, poor management and inadequate laws do not cause corrupt conduct. They only provide the opportunity. The true cause of the development of the illicit trade was the readiness of those who would benefit from it to take advantage of that opportunity; greed and a singular lack of integrity was necessary to a trade built on breach of trust and bribery. That combination was present in several ostensibly responsible major financial and commercial as particularly disappointing and disturbing.

Cause and effect were not hard to find.

Commercial ethics, or the want of them, rank high among the causes of the corrupt conduct revealed. The greatest effect of the corrupt conduct was a gross invasion of personal privacy.

Commercial ethics

Most of the large financial and commercial institutions whose affairs were investigated had, or purported to have, codes of ethics. There was an asserted company policy which was made known to staff, generally by a series of memos or other edicts from above. They were readily available and were offered as evidence to the Commission. In some instances expressly, and in all by necessary implication, they prohibited the use of illegal checks, as the practice of purchasing information obtained by the bribery of public officials was known throughout the industry.

Yet practice and principle rarely matched. The codes of ethics and the express provisions of the ethics memos were regularly breached, frequently at manager or senior manager level. The question is: Were these acts of defiance, or should they be regarded as a better guide than the memos to the true policy and attitude of the institutions themselves?

Evidence given by one senior manager is instructive in this regard.

His company had issued policy documents purporting to forbid the use of illegal checks. Yet he was aware that the company continued to use them, and he himself had ordered one in July or August 1990, about two years after the policy directive was first issued.

In his evidence he agreed there was a conflict between the policy directive and what he saw as the company's commercial interest. It was his decision to favour the company's commercial interest. He was, he said, 'trying to do my job as a Manager for (the company) – the ultimate aim was to reduce their ultimate loss'. That, he said, applied irrespective of the propriety of his conduct.

The next question was whether he, as a senior manager, believed that accorded with the priorities placed by the company on commercial ethics and commercial interests. That was pursued in his evidence, from which I now quote:

> In any such situation you would have to weigh those competing interests, and one you would allow to prevail. Is that right? --- Yes
>
> You couldn't serve them both, because they were in conflict with one another. Is that right? --- That's right, yes.
>
> Now I'm asking you whether what you did when you conducted or obtained these checks was to place the importance of the commercial interest of (the company) as you saw it, above your obligation to comply with the directive? --- Yes
>
> My next question was in doing that did you believe that you were doing what the company required of you in the case of such conflict? --- Yes.

As the ICAC Report records, counsel for the company was understandably anxious to ensure that the witness had followed the questioning and that there was no confusion about his evidence. He was given leave to question him, and did so. After going carefully over the same ground, he obtained this confirmation:

> Now you said, I think, in answer to the Commissioner's question, that you believed when you preferred what you perceived to be the commercial interests the company to their expressed ethical policy, you were doing what you the company required of you. Is that a fair summation of what you said? --- Yes

That was a senior manager.

In the case of one bank, senior managers contradicted one another and were separately represented for the purpose by different Queen's Counsel as they sought to shift responsibility from one to the other.

The implications for personal privacy

Personal privacy was a casualty of the corrupt trade, as addresses, criminal records. social security particulars, overseas passenger movements and silent telephone numbers all became open secrets. A considerable amount of argument was heard from commercial interests claiming a right to the information, and privacy watchdogs who urged resistance to the demands for greater access to personal records for commercial purposes.

It is obviously necessary that there be a clear policy with regard to the availability of personal information held by government departments and agencies, either to the public generally or to special interest groups. I took the view that determination of that policy is not a matter for the Commission. What the Commission could properly do, and did, is point to possible corruption implications of the policies that might be considered.

Attention was drawn to the following among other matters.

- There are dangers in allowing access to special groups or for special purposes only.
- On the evidence of their conduct as revealed by the private investigators they have little claim to privileged access.
- Ready access to information can destroy the market for a corrupt trade.
- If confidentiality cannot be ensured, the accuracy of the information to government departments and agencies is likely to suffer.

The basic privacy principle involved is that when information is provided under compulsion or in confidence, it should be used only for the purpose for which it was given, and it should be available only to persons who need it for that purpose That principle has to yield, however, where it conflicts with a greater public interest such as the interest in the proper investigation of serious crime. A critical question is what circumstance should be allowed to prevail over that basic privacy principle.

The recommendations

Weakness in both management and the law are addressed in the recommendations made in the ICAC Report. Those recommendations reflect the findings and the implications of those findings, as here today.

Many of them call for action at Government level, and there are proposals for legislative change. There are also recommendations for review of departmental practices.

So far as systems and management are concerned, they are of course matters calling for special expertise to which I make no pretence. However, the nature of the shortcomings that were identified enabled recommendations to be made in general terms.

In summary, they are:

- that a policy be developed in respect of all government-held information ... to determine what information is to be publicly available and what is to be protected;
- that all information which is available to the public be made readily, and cheaply available;
- that security of all information storage and retrieval systems be constantly and where necessary updated and improved; and
- that access to protected information be strictly limited, and an efficient system maintained to enable the persons responsible for all accesses to be identified

Recommendations for review of the law included:

- that unauthorised dealing in protected government be made a criminal offence;
- that law apply consistently to information held by all government departments and agencies;
- that attempts be made to have legislation along the lines suggested adopted as the basis of uniform laws, or at least consistent laws, throughout the Commonwealth, and
- that urgent attention be given to the need to amend the law relating to and official corruption in New South Wales.

It was recommended that criminal sanctions in the data protection legislation should cover all unauthorised dealings, without it being necessary to establish the means by which the information was obtained. The sanctions must apply at every point in the distribution chain.

There were recommendations arising from the participation in the illicit trade by commercial and private inquiry agents, major financial institutions and some solicitors. They can be summarised as follows:

- that there be a thorough review and overhaul of the law relating to the and practice of commercial agents and private inquiry agents;
- that consideration be given to revising the law relating to the criminal; and

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

In addition to the matters already referred to, recommendations were made for amendment to the *ICAC Act* itself, in the light of what are to be inappropriate requirements imposed upon the Commission, particularly with regard to findings of corrupt conduct and expressions of opinion related to possible prosecutions.

The fundamental proposition on which the recommendations were based is that the Commission should retain its full powers as a fact-finding body, but should not be called upon to make decisions of law:

> In any findings made by the Commission, it is the facts that are important rather than a decision that the conduct disclosed falls on one side or the other of an artificial line drawn by the law. (ICAC Report, p. 89)

Recent litigation arising from ICAC determinations on technical questions of law and construction – largely, arguments on the meaning of words – illustrate the damage that can be done to the Commission and its standing when it is drawn into such areas.

And one year on

Recommendations made by the ICAC have not always received appropriate attention, especially when action by Government or Parliament is called for. Attention was drawn to that fact in the Report on the Unauthorised Release of Government Information. Some earlier recommendations were repeated, and a plea was made for urgent attention to the matters raised. I quote from the Report:

> One benefit of Commission investigations and Reports, is that they can touching integrity in the public sector. Those Issues can be more important than the particular facts and circumstances that bring them to light. The investigations and Reports would be of more value, I believe, if there was more serious debate about the issues and less preoccupation with the individuals whose conduct is under consideration. The community may feel it is entitled to look to the Parliament for leadership in that regard.

It is interesting to note how different people have responded to the matters disclosed in the course of the investigation and in the Report. The attitude adopted by some is encouraging. With others, there is still cause for disquiet.

A necessary first step to setting matters right is to acknowledge that there is something wrong.

The responses of the New South Wales Roads and Traffic Authority and the Commonwealth Department of Social Security to the findings of the Commission provide an interesting comparison.

In October 1992 the Chief Executive of the RTA spoke at a public seminar organised by the Commission. He acknowledged that bureaucratic delay had encouraged people to go to 'other channels'. He went on:

> There are people in the organisation who are prepared to release that for personal gain ... That trading in information has been much facilitated by poor custodianship.
>
> There have been rudimentary systems, or control of systems. There has been lack of security. There has been poor management. There has been inadequate expression of the ethos of the organisation in its stand corrupt activity.

That was the Chief Executive talking about his own department.

Accompanying that acknowledgment have been a series of appropriate responses. Movement to a highly sophisticated data processing system was already under way while the Commission's investigation was in progress. Full logging audit trails and monitoring those trails are among the security measures. Third party access has been greatly reduced. Agreements and appropriate undertakings are being obtained from the now limited number of third party users. Training sessions, discussion groups, internal publications and a recently developed video are all part of a campaign to change attitudes and culture.

The Authority works closely with the ICAC's own Corruption Prevention Unit.

In addition, firm action was taken with officers found to have engaged in the illicit trade. Two had resigned shortly before the investigation began. During the course of the investigation two others sought to resign, but their resignations were not accepted. After they made serious admissions to the Commission, they were dismissed. Of eleven others found to have sold information, ten were dismissed and one was reprimanded.

Compare that with the reaction of the Department of Social Security.

There has been some playing at the edges with the criminal sanctions contained in the relevant legislation. And it may be that steps to achieve greater security have been taken within the department. That I don't know. What concerns me is the apparent unwillingness to acknowledge the extent of the problem.

Let me explain.

Following the ICAC Report, the House of Representatives Standing Committee on Legal and Constitutional Affairs began an inquiry. One of its Terms of Reference was to examine the ICAC findings. It was to report on the implications for information handling practices in Commonwealth administration. I gave evidence before that Committee. In the course of that evidence, I explained that although the ICAC investigation was necessarily concerned with matters affecting the New South Wales public sector, it had come upon some information relevant to the Commonwealth and relevant in particular to the subject of the House Committee's Inquiry. I said that what had been incidentally discovered warranted the conclusion that there had been an enormous leak of information from the Department of Social Security.

That did not please the then Minister for Social Security. Within hours of my having given that evidence, a spokesperson for the minister said that my conclusion was unfair and unreasonable. It was unfair and unreasonable, he said, because the minister had been advised by the Director of Public Prosecutions that the ICAC findings would justify two prosecutions only.

Perhaps nothing could better illustrate the difference between the effectiveness of a body such as the ICAC and the effectiveness of the police/court system when it comes to eliciting facts in a matter of this nature. You be the judges as I tell you some of the facts.

- One private investigator who had been selling social security information told the Commission that the cost to him of that information was of the order of $40,000 to $50,000 per year. He had two sources in the department. They were named, they were called, they gave and they admitted they had released the information.

- Found among that private investigator's papers was an order for social security information placed by a bank months after the Commission's had become publicly known. It was one of the bank's weekly orders for social security information from the investigator. It contained requests for information about 46 people. That was one order from one bank to one private investigator. And the information was provided – in February 1991.

- Another private investigator told the Commission that over a two-year period he had netted $90,000 from the sale of some 4,500 pieces of social security information.

- Of the New South Wales private investigators whose affairs were examined by the Commission – and they were but a small percentage of the State's total – there were 50 who were found to have dealt in the Department of Social Security.

- Information found to have been sold by one private investigator included the contents of a Department of Social Security file including correspondence going back ten years.

- A brochure distributed by one private investigator in the 1980s openly advertised his wares. It included the following:

  No 2 check: A search of social security records. This search will ascertain if the debtor is receiving a pension or unemployment benefits. It will give the latest address on record and the date of last payment. This search can be carried out in all States. $20 for Australia-wide searches.

  That private investigator developed and maintained his own database of purchasers in the course of his business. His clients included two of the "Big Four" banks.

- Quite apart from sale, a great deal of information from the department's records was released through the Information Exchange Club. Some reached

> banks and real estate agents. Eight employees of Prospect Electricity and five employees of Sydney Electricity told the Commission they had obtained social security information in that way. Between them, they named a total of 16 officers of the Department of Social Security as being involved in the release of that information to them.

If the Minister for Social Security believes it is unfair and unreasonable to describe as enormous the extent of information leaks from the department indicated by that material, there are grounds for grave concern as to the seriousness with which the problem is regarded.

I can brighten that picture a little by saying I am encouraged by the response of the Commonwealth Attorney General. Mr Lavarch was of course Chairman of the Standing Committee on Legal and Constitutional Affairs which was considering the matter and which died with the last Parliament. A new Committee has now been appointed, and the Attorney has referred new Terms of Reference so that the Inquiry may continue. He has written:

> I hope that the inquiry will yield recommendations for future comprehensive reforms on the protection of third party information held by the Commonwealth.

That interest shown by the Commonwealth is hopefully a good sign for the prospects of uniform legislation on data protection.

The New South Wales Police Service, like the Roads and Traffic Authority, has tightened systems and is working closely with the ICAC. Also like the Roads and Traffic Authority, it has taken the disclosures of corrupt conduct involved in the unauthorised release of confidential information.

Stimulated by the ICAC investigation, police carried out their own check on the security of their computer system. They acknowledged at the Commission seminar last October that they found it 'lacking in some areas', in particular with regard to password security and audit trails. New arrangements and rules are now in place. I understand they are being stringently enforced.

Before the Report was published, twelve police officers later named in it had been suspended or had resigned. They ranged in rank up to Detective Senior Sergeant.

A positive response

Indeed the response of the New South Wales public sector generally to the call for attention to Information security has been positive. The Office of Public Management in the Premier's Department launched a series of policy and procedure statements in 1991, and is continuing the process. Consultants have been engaged to prepare a draft Statement of Best Practice on Information Security Management.

As representatives of those consultants will be speaking later this morning, I make no further reference to their work, beyond observing that the Office of Public Management has advised that the proposed Statement will recognise the recommendations of the ICAC Report, and that an exposure draft is expected to be completed by August 1993.

What of the ultimate purchasers and users of the information – the commercial and financial institutions?

The worrying aspect with regard to them is not defective systems or management. It is ethics. I probably place greater emphasis on ethics than Alan Rose indicated he does when he spoke yesterday of values and ethics. After all, defective management and defective systems don't cause corruption; they only provide the opportunity.

I have already referred to the senior manager of a finance company who told the Commission that he believed his company expected him to prefer its commercial interests when they conflicted with its professed ethical standards. Another illustration that is available shows a finance company's response to admitted improprieties by a senior employee.

Do they really care?

An upper middle rank officer in a finance company admitted ordering and obtaining improperly released information directly from public officials whom he agreed to pay for the information. He had then arranged for a private investigator to make the payments in cash on his company's behalf to the public officials and to render false invoices to the company to enable it to reimburse the investigator. In that way he effected a very simple laundering of payments that in real terms were bribes. That went on for five or six years.

When informed by the Commission the company in its initial submission said:

> This company, since its inception in 1982, has an unblemished record of compliance nationally and internationally, with every relevant law or regulation the company prides itself upon its moral essence and does not tolerate any intentional wrong doing.

In a later submission the company contended that there was 'no evidence that this arrangement was carried on by the company as an entity, as distinct from that carried on by Mr (the officer concerned) as an individual'.

How did that company react to the admitted 'intentional wrongdoing' of that officer – conduct which it 'does not tolerate'? When the Commission's Report was being prepared almost a year after the officer's admission, further inquiry was made of the company. It was asked what the position then was so far as that officer was concerned. The answer? He is the company's Credit Operations Manager for Australia and New Zealand.

Representatives of the banking and insurance industries spoke at the seminar in October 1992. In their addresses they concentrated on their contention that much of the information that had been improperly bought should be made available to them. Neither reported action along the lines of that taken in the public sector. It was difficult to avoid the impression that the wrongdoing was 'tolerated', because it was done in the interests of the institutions concerned.

The Executive Director of the Australian Bankers' Association referred only briefly to action taken with regard to the disclosed unethical or illegal behaviour. That was not part of his prepared address. It came during question time. He then said

> What they did was illegal. These people are being punished, they've been disciplined within their banks. The banks have put in place procedures to deal with that.

When I was preparing this Address, I invited the Executive Director to let me know if there was anything further on that subject he would like me to refer to when speaking of steps taken by the banks in consequence of the ICAC Report. He wrote

1. Employees have been made aware of the need to comply with the Privacy Act in particular. Using or soliciting unauthorised information result in dismissal in most cases.

2. Mercantile agents used by the banks have been reviewed and made aware of the unacceptability of using or obtaining such information.

3. Legal compliance procedures have been reviewed with the intention of ensuring,

   - Employees have a full understanding of the issues and consequences

   and

   - Compliance with all laws applicable to Banking.

It is to be hoped that the attitude indicated is now being applied and has permeated throughout the relevant part of the private sector. That alone, if it has occurred, might be regarded as justifying the investigation.

The apparent readiness in the past to tolerate and indeed to expect improper and even illegal conduct on the part of officers and other employees, may be largely attributable to the practical exemption from criminal liability the companies themselves enjoyed and probably continue to enjoy, under the *Tesco* principle.

I have no doubt that attitudes and the standard of corporate ethics and corporate conduct will change markedly if corporations and their directors are made more susceptible to the criminal law. Proposals towards that end have been made, and are hopefully receiving active and urgent consideration among the Commonwealth and State Attorneys General.

The Law Society of New South Wales has considered the conduct of its members named in the ICAC Report as having purchased improperly released information.

At the ICAC seminar, the Chief Executive Officer of the Society said:

> The fact is that when people who occupy privileged positions abuse those privileges, and depart from a reasonable conduct, then perhaps the fall is so much greater, and the abuse of trust is so much greater. Regrettably that is what is in this Report.

He went on to say that the Law Society was taking the matter very seriously, and that the conduct of thirteen solicitors in private practice was under investigation

In preparation for today's address I invited the Chief Executive Officer to bring the matter up to date. He replied as follows:

> The various matters arising from your ICAC Report were considered by the Society's Professional Standards Committee, which then reported on all of them to the Council of the Society. In respect of one solicitor the Council has resolved to make a complaint in respect of the solicitor's the Legal Profession Disciplinary Tribunal. In the case of the solicitors, the Society administered a reprimand. In respect the remaining solicitors the Council decided to take no further action.

Where legislation is required

The recommendations for legislative change arising most directly from the findings in the ICAC Report relate to the need to provide adequate criminal sanctions for the unauthorised disclosure and handling of confidential government information.

Data protection legislation was before the New South Wales Parliament while the investigation was proceeding. It was then in the form of a private member's Bill. Since publication of the Report it has been taken over by the Government, and it is now the responsibility of the Attorney General. I had the opportunity of commenting on a first draft last year, when it was hoped that an exposure draft would shortly be given wide distribution.

The latest information made available for the purpose of this Address is that 'it is hoped that an exposure draft Bill will be available for public consultation' shortly. I am advised that:

> ... the legislation by statutory recognition of appropriate data protection principles will provide the basis for a consistent and principled approach by government departments to the issues raised by the Report. The legislation relates in particular to the recommendations made under the headings "Information Policy" and "Information Protection Law", set out in the schedule contained in the Report.

Also arising from the findings in the Report was a recommendation for amendment to the law relating to the private investigation industry.

That is receiving attention

Late last year the then Minister for Consumer Affairs undertook a review of the industry. The review is to take account of a number of matters including the findings and recommendations made in the ICAC Report. An informal call for comments made by the ministry in February 1993 produced 145 phone-in responses from agents, clients, third parties and independent observers.

A discussion paper, I am told, is expected to be issued 'shortly'.

It would be difficult to imagine any recommendation or report by an anti-corruption Commission calling for more concerned and urgent attention from the Government and Parliament than one which points to inconsistencies and uncertainties in the State's criminal law relating to bribery and official corruption. I have already referred to such a recommendation made in a Commission Report in July 1990 and not responded to by the

time the Report on the Unauthorised Release of Government Information was published more than two years later. The opportunity was then taken to remind the Government of that recommendation. We were told that something would be done by the end of 1992.

A discussion paper and draft exposure Bill were produced in December 1992, and comments were invited. Appropriately perhaps, the final day for responses was 1 April.

The draft Bill in my view is totally unsuitable. If it were adopted and became law, the position would be less satisfactory than it presently is. Matters that should have been covered are not. Existing laws that should have been replaced are not. Complexities, with the worst of legalistic gobbledegook, abound in the draft, which introduces convoluted provisions relating to an offender's state of mind. Quite apart from the fact that as a matter of policy they should not be there, they would in many cases be impossible to prove, and would almost defy understanding by juries.

In submissions which I made on the draft, I said:

> I am reluctant to suggest that there has been undue haste or that presentation of the draft is premature, but we still have not had what in my view is the necessary debate about the standards of conduct the community is entitled to expect of its public officials. That is something that should be undertaken before we become involved in the legalistic argument to which the Paper and Bill invite us.

Latest advice obtained for the purpose of this Address is that 'the Cabinet Office with a view to legislation being introduced into Parliament in the forthcoming Budget Session'.

Political donations were also the subject of a series of made in the Commission's 1990 Report on North and Development. The Report called for urgent review and of the law. Like the bribery recommendations, they produced no result in two years. The opportunity for a reminder was taken in the 1992 Report on the Unauthorised Release of Government Information. With almost three years now passed since the initial recommendations, still nothing has been done.

Can you detect the sense of urgency in this advice received from the Cabinet Office just a week ago? It was in response to a request for information for the purpose of this Address.

> ... you raise the question of amendments to the *Election Funding Act*. As you are no doubt aware, the Parliamentary Joint Select Committee upon the Process and Funding of the Electoral System reported in September last year on a range of issues in relation to the *Election Funding Act*. The Government has consulted bodies such as the ICAC in relation to the report, and is yet to finalise its position.

Nobody seriously disputes the proposition that there are two huge loopholes built into the current law. One excludes donations for non-electoral purposes from the disclosure requirement. The other invites concealment of the true identity of the donor. It would take five minutes to draft legislation to overcome the first, and little longer to remove the second. Yet three years has not been long enough. One is entitled to ask, is the will there?

Perhaps the most important recommendations contained in the Report related to the ICAC itself. The object of those recommendations is to preserve the character of the Commission as a fact-finding body, with powers similar to those of a Royal Commission.

I have long campaigned to have the Commission free from the responsibility of saying whether people fit into an artificial category such as that created by the wildly complex definition of 'corrupt conduct' contained in the ICAC Act. I have also pressed for the removal of the requirement that the Commission express all opinion regarding possible prosecution, an opinion that frequently has to be expressed on inadequate information.

Deciding questions of law ought not to be a function of the Commission, particularly questions as barren and as conducive to legalistic quibbling as several that have taken the Commission to the Supreme Court from time to time.

The Parliamentary Committee on the ICAC has recently prepared a report following a series of public hearings on the Commission's future. The Committee's recommendations contain a lot that is good, but some that are worrying.

GOOD The Parliamentary Committee acknowledges that the definition of corrupt conduct is 'overly complex and fraught with difficulties'.

BAD It proposes changes in the definition rather than its removal, although

GOOD When dealing with s. 8 of the *ICAC Act* it questions whether the conduct described in that section 'needs to be defined at all'.

GOOD The Committee agrees that the requirement that the Commission place labels of corrupt conduct on individuals be removed, but

BAD The Committee favours retention of the requirement that the omission make 'statements of opinion' about consideration of disciplinary action or dismissal.

GOOD The Committee reaffirms 'that the ICAC is a fact finding body', but

VERY entertains a proposal that it be limited to the finding of 'primary facts' and has referred to
BAD the Law Reform Commission a number of related questions

Adoption of this proposal could emasculate the Commission and provide a field day for lawyers.

VERY The Committee recognises that 'if the ICAC is to have a long term effect upon
VERY Corruption in New South Wales it is essential that its recommendations be acted
GOOD upon and followed up'. The Committee's follow-up recommendation is an amendment to the Act to require the relevant minister to 'inform the Parliament of his/her response to any ICAC report concerning his/her administration within six calendar months of the tabling of the ICAC report'.

I have probably gone a little beyond my brief. That has been intentional and I make no apology. The intention has been to present the investigation into the unauthorised release of government and the related Report as important both:

- for what it reveals and the stimulus to reform of information handling procedures which it hopefully provides, and

- as evidence of the need for a body such as the ICAC with its full fact finding powers but stripped of inappropriate requirements that it deal with legal technicalities.

Published Reports of the Criminal Justice Commission

Date of Issue	Title	Availability	Price
May 1990	Reforms in Laws Relating to Homosexuality - an Information Paper	Out of Print	-
May 1990	Report on Gaming Machine Concerns and Regulations	In stock as at time of printing of this report	$12.40
Sept 1990	Criminal Justice Commission Queensland Annual Report 1989-1990	Out of Print	-
Nov 1990	SP Bookmaking and Other Aspects of Criminal Activity in the Racing Industry - an Issues Paper	Out of Print	-
Feb 1991	Directory of Researchers of Crime and Criminal Justice - *Prepared in conjunction with the Australian Institute of Criminology*	In stock as at time of printing of this report	No charge
March 1991	Review of Prostitution - Related Laws in Queensland - an Information and Issues Paper	Out of Print	-
March 1991	The Jury System in Criminal Trials in Queensland - an Issues Paper	Out of Print	-
April 1991	Submission on Monitoring of the Functions of the Criminal Justice Commission	Out of Print	-
May 1991	Report on the Investigation into the Complaints of James Gerrard Soorley against the Brisbane City Council	Out of Print	-
May 1991	Attitudes Toward Queensland Police Service - A Report (Survey by REARK)	Out of Print	-
June 1991	The Police and the Community, Conference Proceedings - *Prepared in conjunction with the Australian Institute of Criminology following the conference held 23-25 October, 1990 in Brisbane*	Out of Print	-

Date of Issue	Title	Availability	Price
July 1991	Report on a Public Inquiry into Certain Allegations against Employees of the Queensland Prison Service and its Successor, the Queensland Corrective Services Commission	In stock as at time of printing of this report	$12.00
July 1991	Complaints against Local Government Authorities in Queensland - Six Case Studies	Out of Print	-
July 1991	Report on the Investigation into the Complaint of Mr T R Cooper, MLA, Leader of the Opposition against the Hon T M Mackenroth, MLA, Minister for Police and Emergency Services	In stock as at time of printing of this report	$12.00
August 1991	Crime and Justice in Queensland	In stock as at time of printing of this report	$15.00
Sept 1991	Regulating Morality? An inquiry into Prostitution in Queensland	In stock as at time of printing of this report	$20.00
Sept 1991	Police Powers - an Issues Paper	In stock as at time of printing of this report	No charge
Sept 1991	Criminal Justice Commission Annual Report 1990/91	In stock as at time of printing of this report	No charge
Nov 1991	Report on a Public Inquiry into Payments made by Land Developers to Aldermen and Candidates for Election to the Council of the City of Gold Coast	In stock as at time of printing of this report	$15.00
Nov 1991	Report on an Inquiry into Allegations of Police Misconduct at Inala in November 1990	Out of Print	-
Dec 1991	Report on an Investigation into Possible Misuse of Parliamentary Travel Entitlements by Members of the 1986-1989 Queensland Legislative	Out of Print	-

Date of Issue	Title	Availability	Price
Jan 1992	Report of the Committee to Review the Queensland Police Service Information Bureau	Out of Print	-
Feb 1992	Queensland Police Recruit Study, Summary Report #1	In stock as at time of printing of this report	No charge
March 1992	Report on an Inquiry into Allegations made by Terrance Michael Mackenroth MLA the Former Minister for Police and Emergency Services; and Associated Matters	Out of Print	-
March 1992	Youth, Crime and Justice in Queensland - An Information and Issues Paper	Out of Print	-
March 1992	Crime Victims Survey - Queensland 1991 *A joint Publication produced by Government Statistician's Office, Queensland and the Criminal Justice Commission*	In stock as at time of printing of this report	$15.00
June 1992	Forensic Science Services Register	Out of Print	-
Sept 1992	Criminal Justice Commission Annual Report 1991/1992	In stock as at time of printing of this report	No charge
Sept 1992	Beat Area Patrol - A Proposal for a Community Policing Project in Toowoomba	Out of Print	-
Oct 1992	Pre-Evaluation Assessment of Police Recruit Certificate Course	In stock as at time of printing of this report	No charge
Nov 1992	Report on S.P. Bookmaking and Related Criminal Activities in Queensland *(Originally produced as a confidential briefing paper to Government in August 1991)*	In stock as at time of printing of this report	$15.00
Nov 1992	Report on the Investigation into the Complaints of Kelvin Ronald Condren and Others	Out of Print	-

Date of Issue	Title	Availability	Price
Nov 1992	Criminal Justice Commission Corporate Plan 1992-1995	In stock as at time of printing of this report	No charge
Jan 1993	First Year Constable Study Summary Report #2	In stock as at time of printing of this report	No charge
May 1993	Report on a Review of Police Powers in Queensland Volume 1 An Overview	In stock as at time of printing of this report	$15.00 per set
	Report on a Review of Police Powers in Queensland Volume 2 Entry Search & Seizure	In stock as at time of printing of this report	
July 1993	Cannabis and the Law in Queensland A Discussion Paper	In stock as at time of printing of this report	No charge
August 1993	Report by the Honourable W J Carter QC on his Inquiry into the Selection of the Jury for the trial of Sir Johannes Bjelke-Petersen	In stock as at time of printing of this report	$15.00
September 1993	Report on the Implementation of the Fitzgerald Recommendations Relating to the Criminal Justice Commission	In stock as at time of printing of this report	No charge
September 1993	Criminal Justice Commission Annual Report 1992/93	In stock as at time of printing of this report	No charge

Further copies of this report or previous reports are available at 557 Coronation Drive, Toowong or by sending payment C/O Criminal Justice Commission to PO Box 137, Albert Street, Brisbane 4002. Telephone enquiries should be directed to (07) 360 6060 or 008 061611.

This list does not include confidential reports and advices to Government or similar.