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.