AUSTRALIA'S NEW SOUTH WALES CORRUPTION SCANDAL UNCOVERED

The misuse of personal data for corrupt private gain seems to be endemic and requires the utmost vigilance to be uncovered. We have reported cases in Spain (PL&B Oct '92 p. 3) and in the USA (see p.21 in this issue). In the following report, Ian Temby QC, Commissioner of the New South Wales Independent Commission Against Corruption, describes how the corruption extended to society's most respectable individuals and institutions. It took a powerful and well funded government commission to dig up the dirt. How would other countries tackle the problem?

An Independent Commission against Corruption (ICAC) investigation found a multi-million dollar trade in confidential information from Local, State and Commonwealth Government records, involving hundreds of people as well as some of Australia's better known financial institutions. The Commission's Report, published in 1992, has generated enormous interest, both nationally and internationally.

The investigation began quietly enough. Within two years it had burgeoned into the biggest investigation the Commission has ever undertaken, with wide-ranging implications across the public sector and community generally.

The Beginning of the pursuit

In May 1990 the Police Internal Affairs Branch executed a search warrant on the premises of a private inquiry agent, Stephen James, in Rose Bay, Sydney. This warrant was executed after a lawyer presented to a court a computer print-out of a criminal history form. The supply of this form was traced to Stephen James.

In the search, police seized more than 500 files, the majority of which contained print-outs from computers at the *Roads and Traffic Authority*, or *Police*, or both.

Information so obtained had been passed to over twenty *legal firms*, as many *insurance companies*, and several *banks*. Criminal history print-outs had either been sought and/or received by thirty different legal firms, twenty six insurance companies and four banks. Payments for the service were documented.

Personal data traded

The Police Service notified the Commission by way of a Section 11 report, which is compulsory under the ICAC Act if corruption is suspected. The Commission had the powers and the desire to pursue the matter. After preliminary inquiries, a formal investigation was begun in May 1990. In July of that year Assistant Commissioner Adrian Roden QC was assigned to the matter. Public hearings began in November 1990 and continued until early 1992.

It became obvious as hearings proceeded that the sale or exchange of confidential information was a massive, lucrative business. Organised networks had developed whereby this information was swapped, bartered or sold.

The information traded included silent telephone numbers, addresses, passport particulars, bank account details, pension details, criminal histories and immigration information. Typically the information was released by a State or Federal Government public official to a private inquiry agent or commercial agent. The information was usually used for their purposes on behalf of a client but sometimes it was sold to another agent.

Corruption and concealment

The finance, banking and insurance industries embraced the practice. Indeed, the mammoth proportions it reached can be attributed largely to the involvement of these industries. Often an insurance company, bank or other financial institution ordered the information from the agent knowing how it would be obtained, or at least knowing that

there was no legitimate way of obtaining what was sought. *Solicitors*, some of them officers of public sector institutions, also engaged in the trade usually through a private inquiry agent.

Elaborate methods were used to conceal the trade. Between some agents and banks, codes or other elaborate devices were used to conceal the nature of the transactions between the two. Some finance and insurance companies directed the agent to avoid all references to the illegal checks appearing on invoices and reports. Some agents were directed to falsely state the source of the information in their reports.

The investigation identified dozens of people involved in providing confidential information such as police officers including a Detective Senior Sergeant in charge of detectives, staff of the Roads and Traffic Authority, officers of the *Sydney Electricity* body, and *Commonwealth public servants*.

A total of 155 people and organisations were found to have engaged in corrupt conduct with a further 101 found to have engaged in conduct which allowed, encouraged or caused corrupt conduct.

Some public officials were only occasional sellers of information but others were heavily engaged in the practice and had been for some years.

As we know, knowledge is power and human nature being what it is, the levels of ingenuity exercised by individuals in the accumulation and dissemination of confidential information is not too surprising. What is surprising, though, is the extent of that dissemination.

The information exchange club

Of particular note is a mechanism whereby information was exchanged, or that exchange was facilitated. This was the Information Exchange Club where contracts were made at social functions organised for the purpose of swapping information, apparently with departmental approval. Admission to the Club was extended to include staff from banks and other financial institutions.

One woman who had access to the Club through a previous job with a finance company, used it to get addresses of electricity consumers to sell them to a private investigator. She also developed a trade in *Telecom and Social Security information*. In exchange, she gave information obtained by her, in her employer's name, from the *Credit Reference Association of Australia*.

Another example: a private investigator used an officer of Sydney Electricity to get information on overseas passenger movements. The officer got that information through the Information Exchange Club from people in the *Department of Immigration* or the *Australian Customs Service*.

In another case, a police officer used the personal access codes of four other police officers to obtain information from the Police computer. The police officer eventually admitted dealings with seven private inquiry agents, including a former NSW police officer, a former *New Zealand police* officer and a former solicitor. One of them gave him a facsimile machine to install in his home to more easily provide information.

And around and around it went.

One one occasion, a private inquiry agent invoiced a client for his services in providing information. Included on the invoice was the entry "*Corrupting police*"!

An *unlicensed private investigator* was caught in the act of buying confidential information a few weeks after he had denied in the witness box ever being involved in the trade. In fact, he had been a major dealer for more than ten years.

Many private investigators involved in the trade are former police officers. It was relatively easy for them to establish a network with their former colleagues to facilitate the sale of police documents and the release of large amounts of confidential information onto the illicit market.

Cost of corruption passed to consumers

The sums of money involved in the sale of information ranged from a few dollars for each

"check" to hundreds of dollars for some individual efforts.

Some public officials earned over $100,000. The private inquiry agents would pass that cost on to their clients, together with something extra for themselves. Presumably in many cases *consumers were, in effect, paying or reimbursing financial institutions for invading their privacy.*

Of course these ill-gotten gains were not made known to the Tax Office. Taxation assessments totalling more than $2 million have since been issued.

No policy coordination

While individuals have been the main perpetrators of the trade in information, the institutions for which they worked must accept some responsibility.

Statements of policy from public authorities to the Commission demonstrated a lack of consistency, which could be expected in the absence of a coordinated policy. Some public officials were genuinely unaware of what information they could properly disclose and to whom they could disclose it.

The Commission's investigation, dealing mainly with the NSW Government but also some Federal Government departments, uncovered a practice that was entrenched in *public sector culture*. It would be naive in the extreme to assume that the practice was not carried on in other States, and at Federal level. The information sought is of great value to many.

It is heartening at this point to note that the Federal Government's *House of Representatives Standing Committee on Legal and Constitutional Affairs* is currently conducting an inquiry into aspects of the ICAC's report which involved Federal Government departments.

Information available to anyone with money

What the investigation has disclosed is that the Australia Card debate of several years ago was very much a theoretical one. It is now clear that the trade in supposedly confidential government information was simply privatised. Through corrupt officials the information went out to the private sector. It has been available to anyone who has got the requisite amount of money and/or the right contacts. The situation cannot continue and proper, effective, remedial action is called for.

Why have the revelations been exposed now?

The answer is not that New South Wales has a unique problem. Rather it has a unique institution - an independent body which is empowered to investigate matters such as this and given the necessary resources, powers and functions to do so.

It is very clear that had there not been an Independent Commission against Corruption, then none of what we now know which is so very important to the public would have become known. Had it not been for the Commission, then quite clearly what started off as a police task would have remained so. The result may have been the laying of a charge against one or two individuals, but it is absolutely inevitable that the trails could not have been pursued. People would have simply insisted upon their right to remain silent and not name their sources.

It was only because a Commission existed, which had the powers, and desire to investigate, that we were able to take the necessary steps to find out exactly what had been going on. Through the Commission's work the problem area has been identified, exposed, measured and reported upon.

Clearly the law was broken, or disregarded. The privacy of individuals was invaded in a systematic way. The relationships betwen public officials and people in the private sector led to and fed the practice of selling confidential information.

The report's recommendations

The report highlights the need for *urgent reform of the criminal law* in relation to unauthorised dealings in government

information. It recommends a thorough *review and overhaul of the private investigation industry* and consideration of the principles of law governing the *criminal liability of corporations and the responsibility of directors.*

Recommendations are also made for the *government to develop policies* to determine what information should be publicly available, and what should be protected, and effective procedures for the implementation of these policies.

To quote from the Report:

"If the corrupt trading is to be kept in check, three things are necessary:

1. There must be a clear line drawn between information which is available to the public, and information which is retained as confidential.
2. That which is available to the public, should be readily, quickly and cheaply available.
3. That which is to be retained as confidential, should be properly protected."

There has not been any consistent policy in relation to what information should be available to the public. Access to publicly available information has been subject to delays to such an extent that a quicker, more efficient illicit trade in the sale of information has sometimes evolved. Where there is demand, there will be supply.

Multiple Access Points

Confidential information has not been well protected, particularly within the Roads and Traffic Authority and the Police Service where there are multiple access points to large databases. If information is to be kept secure, this multiple access question must be properly addressed. Fortunately steps have been taken by the departments named to provide a *secure, detailed audit check system* for access to their databases.

If technology can provide an answer, well and good. But this of itself, would not be enough. There must also be correct measures at an *organisational level* and a *legislative level.*

If technology cannot solve the multiple access problem, then we either accept the proposition that none of us have any effective right to privacy, which would be a dismal conclusion, or the *community must demand that the government ceases to gather so much information about its citizens.*

Categorising information as confidential

The whole question of how information should be categorised is a complex one. I don't pretend to have the answers and indeed, this is a policy issue for others to decide.

Information categorised as being confidential accordingly grows in value and serious questions have to be asked as to whether too much government information, including information about individuals, is being given that confidential label.

We would ignore at our peril the considerations placed before us by both those involved in debt collection and bankers, insurance companies and so on, on whose behalf debts are collected. Their talk about the values inherent in a settled society are not to be scoffed at. Their arguments need to be borne in mind.

But it is an over-simplification of the issues to state that personal information is needed for "good" purposes such as tracking down debtors, therefore the information should be made available legally.

The personal information sought has sometimes pertained to family members other than the debtor. And the information is sometimes used for more sinister purposes. Obtaining information improperly can hide deficiencies in the "proper" system, due to lack of use.

Neeed for clarity for disclosure criteria

It seems to me in deciding what information about individuals should be made available we must take into account the nature of the information in question and the type of

information we are dealing with. Also we must be aware of the basis on which it is obtained, most obviously, whether it is volunteered on the one hand or demanded on the other. And one must have regard to the purpose for which the information is sought. It seems to serve the public good to make information available for legitimate law enforcement purposes.

However, if information is to be made available for law enforcement purposes, it must be taken to ensure it does not mean that any one of 15,000 police officers in this State can get it simply by identifying themselves as a police officer and saying they need it for the performance of their functions. Without wishing to denigrate the great mass of honest police officers, the simple fact is that some of them cannot be trusted with our secrets.

Accordingly, one needs to ensure that steps are taken that the particular officer has a need to a particular context and that the information, once obtained, cannot be thereafter easily abused or let into general circulation. And there must be clarity as to the rules that apply. Having formulated rules according to decided criteria, they must be clear.

That can be done by legislation, because legislation is publicly available and everyone can know what it entails. Alternatively, if the rules are determined administratively it is essential that there be a full disclosure of what those rules are.

If public bodies have information about individuals and to the extent that they deal with that information, they should be prepared to disclose the basis upon which they are doing so. In case of reluctance, they should be required to do so, the most obvious vehicle being by stating their policy in their annual report.

Conclusion

Our job in relation to this investigation is almost complete, save for pushing for reform in a number of areas. Presently there is *no direct criminal offence in relation to the unauthorised release of confidential information.* Tighter controls of the private investigation industry are needed. There needs to be new laws in relation to criminal liability of corporations.

It is not the Commission's function to resolve the debate over maintaining privacy of personal information and the claim by some in teh commercial world and elsewhere for access to that information for their commercial purposes. That is the role of the Privacy Commissioners.

This edited report was presented at the 14th Annual Privacy Commissioner's Conference, Sydney, Australia, in October 1992, by Mr Ian Temby QC, Commissioner ICAC, NSW, Australia