REMOTE ACCESS INFORMATION DEVELOPMENTS

SEMINARS: BRISBANE, MELBOURNE AND SYDNEY

MARCH 1979

PRIVACY PROTECTION, ECONOMIC PROTECTIONISM

The Hon. Mr. Justice M.D. Kirby

Chairman

Australian Law Reform Commission

March 1979

REMOTE ACCESS INFORMATION DEVELOPMENTS

SEMINARS: BRISBANE, MELBOURNE AND SYDNEY

MARCH 1979

PRIVACY PROTECTION, ECONOMIC PROTECTIONISM

The Hon. Mr. Justice M.D. Kirby

Chairman

Australian Law Reform Commission

THE INVOLVEMENT OF THE LAW REFORM COMMISSION

The first question that may legitimately arise is how a group of lawyers, and specifically a judge, come to be involved in the developments concerning the remote access to information.

The Australian Law Reform Commission was established in 1973. Its first members were appointed in 1975. It works upon references received from the Commonwealth Attorney-General, Senator Durack.

A common theme of a number of references given by successive Attorneys-General has been the endeavour to update the law and to face up to the challenges posed by developments of technology. Our report on Human Tissue Transplantation is an example of the way in which it was necessary to modify the common sense and Common Law definition of "death" in order to recognise the development of ventilator equipment in hospitals. Similarly reform of the law of defamation requires acknowledgement of new forms of spreading information, e.g. broadcasting, television, telefacsimile and the like. The reform of criminal investigation law requires the use of the telephone to permit judicial superintendence of certain police decisions. It also suggests the use of tape recording to set at rest some of the disputes concerning confessional evidence.

It is the reference to the Law Reform Commission on privacy protection that specifically brings us together. That reference requires the Commission to produce a report which will propose new laws for the protection of privacy in Australia. The Common Law has generally failed, in our country, to develop laws for the protection of privacy. Various statutory provisions exist both at the Commonwealth and State levels but, generally speaking, they are piecemeal and unsatisfactory.

It is the development of computing (and specifically computing in conjunction with telecommunications) that has caused all Western democracies to re-examine their legal systems, with a view to the provision of new laws for "privacy protection" or, as they call it in Europe, "data protection".

It is the capacity of computing to collect vast masses of information, store it indefinitely, retrieve it at ever-diminishing cost and ever-increasing speed and in a form that is not easily understood by the layman, that calls for new methods of legal control. The Law Reform Commission's task in the Federal sphere in Australia is not a unique one. Similar tasks have been assigned to various State bodies, including State Law Reform Commissions in Australia. As well, throughout the Western world, governments have set up committees and, in many cases, enacted legislation to provide their citizens with adequate data protection.

In the future, people will not invade your privacy or spy upon you so much through the keyhole as through information systems. The aim of legislative data protection is to ensure that, in the midst of dramatic technological advances, we do not lose sight of the importance of the individual human being and his right to define certain aspects of his personality as private and deserving of protection.

The Law Reform Commission is proceeding to its report in a number of stages. In a few weeks it will deliver a report on Unfair Publications dealing with privacy protection in publication of private facts, particularly mass publication. Also in a few weeks

the Commission will be putting out a discussion paper on privacy and the census. The census is being taken as an example (and an urgent example) of the need for adequate privacy protection. It is the universality and compulsory nature of the census that calls for particular attention. It is the advent of the 1981 census that calls for urgent attention by the Commission.

Later in the year, the Commission hopes to publish discussion papers dealing with the whole question of informational privacy generally. It is here that we will have to call attention to the overseas legislation and draw lessons for Australia from the developments beyond our shores. It will also be important for us to fit our privacy protection into the context of our own social values and legislation already passed or presented to Parliament. The Ombudsman Act, the Administrative Appeals Tribunal Act, the Administrative Decisions (Judicial Review) Act and the Freedom of Information Bill all provide valuable, important, novel rights of access to information by Australians. They are limited to the public sector but they represent an important advance in the right of the individual to have information, including information about himself. The Australian Law Reform Commission's project is limited to the Federal sphere in Australia. However, we are working closely with State colleagues and hope to produce a report that will be of general use to the whole Australian community.

WHY TELECOMMUNICATIONS?

There are two reasons why lawyers have a particular interest in the telecommunications aspects of information systems. The first is the close integration of the technology of computing and telecommunications. I do not need to elaborate this to the present audience. The second is specifically a lawyers concern. Many businessmen, manufacturers, lawyers, governmental officers and others have emphasised to the Law Reform Commission the inconvenience that would arise if there were differing approaches to data protection law in Australia. The integration of our telecommunications system and the increasing dependence of computers upon the telecommunications system makes the possibility

of differing standards and different machinery in the 6 States and 2 Territories of Australia an unthinkable legal nightmare. It is for that reason that we are endeavouring to develop principles that will be generally acceptable by the Commonwealth and State Governments alike. In addition, it is natural that with the pressure for a single uniform law throughout Australia, Commonwealth officers should look to the powers they have under the Constitution of the Commonwealth. When the Constitution was drawn no specific power was given in relation to computers, for obvious reasons. Nor was power given in relation to privacy or data protection or information systems. These matters, therefore, would normally remain with the States. One power given to the Commonwealth under Section 51 (v) of the Constitution is a power to make laws with respect to postal, telegraphic, telephonic and other like services. It is therefore important for lawyers, particularly those concerned with the design of laws for data protection, to look closely at that power and to see whether it provides the mechanism for avoiding some of the disparities in data protection laws that already bedevil European countries. We should not want our continent to become the repository of inconvenient and differing data protection laws which provide a real impediment to the free flow of information, which legitimately may be required, from one end of the nation to the other.

WHY THE O.E.C.D.?

Australia is a member of the Organisation For Economic Co-operation and Development. The headquarters of this organisation are in Paris. The organisation numbers 21 countries. Basically, they are the democracies of Western Europe, North America, Japan, Australia and New Zealand. These countries have many things in common, including the desire to encourage and promote the expansion of international trade and the exchange of information between similar countries.

For several years now the O.E.C.D. has been closely examining the laws of data protection and privacy protection, as it is called in the English-speaking world. The reason for the interest of an organisation which is primarily economic in bias is the recognition of the fact that differing privacy protection laws and differing standards and machinery for enforcement will, potentially at least, create barriers against the free flow of information between member countries. The fear is that conditions will be imposed upon the exchange of information that will prevent the free flow of such information. This, then, is the legitimate concern of the O.E.C.D.

This international organisation is not, however, the only international body that is looking at the harmonisation of domestic privacy protection laws. The Council of Europe has established a committee of experts which has almost agreed upon a draft convention that will be available for signature by the countries of Western Europe. As well, the Commission of the European Economic Community is examining the question of whether a directive should be given to the Governments of the Nine to bring their data protection laws into close harmony. The European Parliament is also examining data protection, as is the Nordic Council, U.N.E.S.C.O. and the United Nations. Our link in Australia, with this international movement towards the rationalisation and harmonisation of privacy protection laws, is through the O.E.C.D.

Putting it bluntly, the fear expressed in a number of the international organisations is twofold. First that, with the best will in the world, domestic approaches to privacy protection will inevitably differ and thereby create barriers and impediments upon transborder flows of data, including personal data. Secondly, the fear is expressed in some quarters that, in the name of privacy protection, legislative measures will be passed which will have a very real impact to restrict the free flow of information between countries. In this connection, it is feared that economic protectionism, national sovereignty and pride, fears as to the vulnerability of overseas data processing, concern about the loss of employment to overseas data processers

and concern about loss of technological experience, will all lead to the creation of data protection machinery which impede the free flow of information throughout the world. In other words, the fear is that legislation will be developed in some countries which is avowedly to protect the privacy and individualism of citizens of those countries but is in truth enacted in order to protect other national values such as employment, technological excellence, sovereignty and so on.

THE O.E.C.D. MANDATE

It was in this context that the O.E.C.D. established an expert group of intergovernmental experts with a mandate to look into a number of aspects of the implications of free flow of information between nations. The mandate or terms of reference to the O.E.C.D. Expert Group is important and I shall set it out in full:

> "(i) Develop guidelines on basic rules governing the transborder flow and protection of personal data and privacy, in order to facilitate a harmonisation of national legislation, without this precluding at a later date the establishment of an international convention; and
>
> (ii) Investigate the legal and economic problems relating to transborder flow of non-personal data in order to provide a basis for the development of guidelines in this area which should take into account the principle of free flow of information."

The Expert Group is instructed to report on item (i) of its mandate by 1 July 1979. It is instructed to carry out its work "in close co-operation and consultation with the Council of Europe and the European Community". This latter instruction represents a recognition of the fact that there is a close similarity in the personnel working withing the O.E.C.D. Expert Group and personnel who comprise the Committee of Experts of the Council of Europe.

The Expert Group has met on a number of occasions in Paris and Stockholm. It has established a Drafting Group and has appointed a consultant to work to the Groups. In addition to this international procedure, we in Australia, through the Law Reform Commission, have held two national seminars to consider the draft guidelines on item (i) of the mandate, in order to ensure that they are in line with our domestic requirements and interests. The next such seminar (the third) will be held in Canberra on 8 May 1979.

PROGRESS IN THE O.E.C.D. GUIDELINES

The last meeting of the Expert Group in Paris identified a number of specific issues upon which the O.E.C.D. member countries differed. For convenience I list those issues now:

(a) Whether the guidelines should be limited to A.D.P. systems or should govern information systems generally.

(b) Whether the guidelines should be limited in terms to natural persons or should extend, as the legislation in some European countries does, to legal persons as well.

(c) Whether there are any categories of "specially sensitive data" that can be defined and require special treatment. The Europeans, with the memory of the last War fresh, urge that there are some categories of information which should be given specially protective treatment. They mention, for example, personal details about a person's religion, philosophical views, political persuasion, racial origin and so on. The United States participants take the view that it is the context and use of information, rather than its nature, that leads to sensitivity and that it would be difficult to get agreement, between the different cultures represented, as to just what was the specially sensitive data.

(d) Whether the guidelines should extend only to member countries of the O.E.C.D. or should be available for the benefit of non-member countries of the O.E.C.D. as well.

(e) Whether the various forms of machinery for the enforcement of the guidelines should be spelt out in any detail. Certain items of machinery are generally agreed. The golden thread which runs through the data protection laws of Western Europe is the right of the individual to access to his own data for the purpose of checking whether the data about him is accurate, complete, up-to-date and relevant. But other machinery items see division of opinion. These include the right to erasure, rather than annotation of the record, the right to a copy of information about a person and the right to have reasons where information is denied.

THE THIRD DRAFT GUIDELINES

The O.E.C.D. Expert Group has basically settled the third draf of the guidelines. This draft has still to be put into proper form. It would not be appropriate at this stage to mention its fu details. However, the broad outline can be described. The guidelines will be divided into 3 sections:

(a) Introduction.

(b) Basic principles for the protection of personal data.

(c) Implementation.

The guidelines w l apply to personal data which, either because of the manner n which it is processed or because of its nature and context, p se dangers to the protection of privacy and individual liberties. This formula seeks to marry the approaches proposed by the Europeans and the United States. The guidelines will also apply to the public and private sectors. They will not

exclude the provision of more protective provisions for privacy protection. They will not limit countries from providing that they should apply only to A.D.P. systems. There will be provision for exceptions on the grounds of national sovereignty, security and public policy and otherwise exceptions should be as few as possible, consistent with law and publicly available. The guidelines are to be a minimum standard.

That part of the guidelines which is of the greatest interest to us in Australia is the part which collects the so-called basic principles for the protection of personal data. These basic principles, if agreed upon by the countries of Western Europe, North America, Japan and the Antipodes, will probably find reflection in our own local privacy protection (data protection) laws when developed

The principles include:

(a) Collection limitation: That there should be limitations on the collection of personal data, that it should be collected lawfully and fairly and, where appropriate, with the consent of the data subject.

(b) Information quality: The personal information should be relevant to the purpose of the collection, accurate, complete and where necessary kept up-to-date.

(c) Disclosure limitation: That personal data should not be disclosed without the consent of the data subject or authority of law or other appropriate authority.

(d) Security safeguards: That personal data will be given reasonable security protection.

(e) Openness: That a general policy of openness will be maintained in respect of developments and practices relating to personal data and means will be available for the data subject, or a person suspecting that he is a data subject, to identify the controller of persona data, in order to be able to exercise their rights and work the principles.

(f) Individual participation: This is the critical provision. The guidelines will include a confirmation that a person is entitled to participate in information systems in the following ways:

i) To confirm whether or not he is the subject of information collection.

ii) To have communicated to him data about himself quickly and at a cost, if any, that is not prohibitive.

iii) That he will be entitled to have the reasons for the refusal of access to his own data.

iv) That he will have a means of challenging data and, where appropriate, to have personal data about him which does not comply with the guidelines erased, rectified, completed or amended.

(g) Accountability: That means will be provided for a person to be identified who is the "data controller" and who is accountable for compliance with the guidelines.

The guidelines will also contain other principles relating to the free flow of information between countries and limiting restrictions on the free flow to that which is reasonably necessary for the protection of privacy. Countries will agree to take steps to implement the guidelines, to take them into account in domestic legislation, to avoid unjustified obstacles to transborder data flows of information and to determine an international mechanism to ensure free flows of information, in balance with legitimate privacy protection.

This then is the progress that has been made in respect of the protection of personal data and the assurance of free flows of such data. This is not just an academic exercise. Nearly half the O.E.C. member countries have already produced data protection laws; others, including Australia, are in the process of doing so.

NON-PERSONAL DATA

A great deal of progress has not yet been made in respect of the protection of non-personal data. This is because the Expert Group has been concentrating on the first item of its mandate in respect of which it has a firm deadline for report.

The thesis which is behind the concern about item (ii) of the mandate was expressed by Mr. J.P. Chamoux in his paper "Typology and Problems" prepared for the O.E.C.D. Expert Group. It is in the following terms:

> "There can be no doubt that once transborder data flows become a significant part of international trade in goods and services they will also attract the attention of tax authorities throughout the world. It is in the interest of all users to give immediate attention to this question in an attempt to reach a consensus at international level. This may be a long and delicate process but it is thought well worth-while to start it without delay. For this reason we put it forward as a subject for study by the appropriate OECD bodies."

It is because of the concern that the massive increases in international flows of data will attract the tax gatherer that the effort is now directed at the identification of ways in which the flows of data between countries can be specified, described, measured and, if possible, evaluated.

Mr. Chamoux in his various studies has identified a number of concerns for the O.E.C.D. Expert Group:

(a) The customs concern: i.e. whether customs authorities will endeavour to find a means of evaluating flows of information for the purpose of adding customs duties at the barrier.

(b) The local tax concern: Whether some form of value-added tax or other form of taxation could be decided which could gather taxation for domestic authorities based upo the rapid increase in the flows of information, which flows have, of course, a great economic value.

(c) Tariff concern: The extent to which telecommunications tariffs need to be readjusted in the light of the rapid advances in technology and the discordancies and inconsistencies that are disclosed in current international telecommunications tariffs.

(d) The nationalistic concern: Whether countries, in the legitimate protection of their domestic technology, the vulnerability of their societies, national pride, employment and so on, impose limitations upon the data processing of certain kinds of information beyond their shores or otherwise limit the movement of certain kinds of information from their countries.

It can be seen that the Expert Group's work here is at a most preliminary stage. Just received is the report of the Logica study "The Usage of International Data Networks in Europe". I attach the conclusions contained in that study.

The O.E.C.D. Expert Group has agreed to the distribution of a questionnaire seeking information from member countries on the way in which an identification of transborder flows of non-personal data can be approached and indication of the way in which such flows can be measured, if at all.

It will be imperative for the Expert Group to have the closest possible assistance of telecommunications and other authorities in the preparation of its report on item (ii) of its mandate. I want to pay tribute now to the assistance I am receiving from O.T.C. Australia and Telecom and various other persons in industry and academic life.

I invite the assistance of all persons engaged in the computing and telecommunications disciplines so that the contribution of the Expert Group can have a distinctly practical bias and can, at the same time, reflect the proper concern of us all to maintain the free flow of information between and among countries to the greatest extent consistent with other competing values. This is not an academic exercise. The world faces

vast changes in technology. Those changes will attract the attention of local lawmakers. It is important that the greatest possible consistency should be brought into the domestic laws of democratic countries so that they do not, by disharmony, unduly interfere in the free flow of information which is to the benefit of mankind.

APPENDIX I

4. CONCLUSIONS

1. The use of international data transmission has produced substantial financial benefits to large multinational companies, airlines and banks.

2. The benefits have been achieved by using company resources more efficiently. Efficient use of resources has been made possible by sophisticated data communications networks.

3. Computer resource sharing is one of the reasons for the initial development of networks and is still one of the most important reasons for data transmission on both a national and international scale.

4. Many of the companies who have taken advantage of the benefits of international data transmission have radically changed their operations, so much that they are dependent on the continued reliability of the service e.g. the world's airlines.

5. The development of international private (leased circuit) networks is a very recent phenomenon and as yet its full potential has not been realised.

6. International co-operation in scientific research and other areas will be stimulated by the development of international data transmission facilities. This has already been demonstrated by the World Weather Watch and European co-operation in high energy physics at CERN.

7. The technological advances of data processing and transmission have created much higher standards of security in information processing than was previously possible. The security of the SWIFT network and the credit control network in this study are much higher than was possible in these applications prior to the implementations of the networks.

8. The more recent development of private switched networks and distributed processing has resulted in much greater reliability of operation and reduced the dependence on individual installations.

9. International data processing and transmission has created a situation of international interdependence, however switched networks are at the same time reducing the attendant risks.

10. However, there will always be some level of international interdependence resulting from international data processing and transmission, and only an international agreement ensuring the free flow of international data can entirely remove the dangers.

11. The most widely used applications over international networks are those relating to company management (i.e. production and stock control, financial planning etc.), banking, credit control and travel reservations.

12. As part of co-ordinated production and stock control applications, some multinational companies hold centralised data files for all their operating companies. This means that data relating to the day to day running of a country's industry is held outside its borders.

13. Most of the personal data transmitted internationally relates to banking, credit control and travel reservations. The level of security has always been high and has become higher with advanced data transmission techniques.

14. Sensitive corporate data is also subject to international transmission. It is often in the form of marketing or sales information held by manufacturing companies about their clients. This data is as sensitive as personal data and should be granted the same protection.

15. The cost of international leased circuit networks is very high, the simplest one-line network would cost about $20,000 per year and most networks in this study cost at least ten times as much.

16. As a result only large organisations can take advantage of the benefits offered by private leased circuit networks.

17. Many organisations such as airlines or large multinational manufacturing companies would not be very sensitive to a substantial increase in the cost of data transmission because these costs are a small part of their overall costs and the benefits achieved are large in comparison.

18. However, other present day users would be sensitive to minor increases in cost, for example banks, whose charge for handling a single transaction is quite small, or computer bureaux who have to equate the circuit costs with the extra business the circuit brings.

19. Increased data transmission costs would also slow down the development of those smaller companies now beginning to use the facilities.

20. Even without increased costs the majority of organisations requiring international private circuit facilities cannot justify the cost. The alternatives to leased circuits, telex or the public switched telephone network (PSTN), are often unsuitable.

21. International telex usage is very expensive compared with bulk data transmission over leased circuits. The organisations in this study are achieving costs of 1 to 10 US cents per 1,000 characters transmitted internationally; within Europe the equivalent telex cost is 60 cents, and to the US much more.

22. The PSTN facilities are poor for data transmission (the error rate is high, the call set-up time is long and it is not sufficiently reliable) and because attainable data transmission rates are low it can also prove expensive.

23. The public switched data networks being implemented should overcome the shortcomings of both the PSTN and leased circuit networks and meet the requirements of all organisations.

24. It is essential that the international tariffs for using these networks should be attractive to allow medium and small organisations to take advantage of all the benefits data transmission offers over other means of international data transportation. The proposed national tariffs indicate a usage charge of about 1 cent per 1,000 characters transmitted.

25. It is unlikely that a European-wide public data network will be available for at least five years.

26. Since organisations have an immediate need for European-wide networks, more private networks will be implemented in the next few years. Organisations also have a pressing need for detailed information on when a European public network will be available.

27. The PTT administrations should therefore continue to offer private circuits at the normal tariffs for several years after the implementation of public networks to enable those organisations to make a gradual and inexpensive transition.