INFORMATION TECHNOLOGY AND SOCIETY

COLLOQUIUM, PARIS

27 SEPTEMBER 1979

COMMISSION 11 : DATA TRAFFIC ACROSS NATIONAL BORDERS

# O.E.C.D. EXPERT GROUP'S GUIDELINES

Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission
Chairman, O.E.C.D. Expert Group on Trans-
Border Data Barriers and the
Protection of Privacy

September 1979

INFORMATION TECHNOLOGY AND SOCIETY
COLLOQUIUM, PARIS

27 September 1979

COMMISSION 11: DATA TRAFFIC ACROSS NATIONAL BORDERS

# O.E.C.D. EXPERT GROUP'S GUIDELINES

Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission
Chairman, O.E.C.D. Expert Group on Trans-
Border Data Barriers and the
Protection of Privacy

## TRANS-BORDER DATA FLOWS

It was once said that my country, Australia, was the greatest international victim of "the tyranny of distance". Not only was this European civilisation distanced by half a world from its cultural origins. Even within the Australian Continent, scattered communities developed, clinging generally to the coastline and on the edge of a vast inland desert. Distance from cultural origins and distance from each other were factors that influenced the early social and political development of the Australian people.

Recent advances in technology reduce the distances both national and international. Whereas it took the First British Fleet, bearing its captive band of unwilling convict migrants, eight months to reach Sydney Cove, I accomplished the same journey by sitting in an armchair for just less than a day.

The revolution in physical movement is dwarfed only by the exponential developments in telecommunications. Now the integration of information sciences by the linking of telecommunications and computers is working the next revolution. It is an international phenomenon. It has consequences for the national security, cultural independence and economic self-sufficiency of all Western countries. It also impacts upon individual human rights, including what we Anglophones have chosen to call "privacy" but what may be better described as "data protection" and "data security".

The key characteristics of the "new information environment created by information technology" have been identified many times. In the Rockefeller Report, National Information Policy, the chief consequences for the United States of the new information technology were identified in terms relevant to most of our countries:

* A massive increase in the volume of information flow: between a four and sevenfold increase between now and 1985.
* A shrinkage of time and distance constraints upon communications. Satellite and other communications provide long-distance capabilities to use computers and other information technology throughout the world at ever-diminishing cost.
* An increase in the inter-dependence of previously autonomous institutions and services, including an increase in the dependence by national institutions upon data banks in foreign countries.
* Conceptual changes in economic, social and political processes induced by increased information and communications. A prime example of these is the impact of the "cashless" society as a result of electronic funds transfer.
* The decrease in the "time cushion" between social and technical changes and their impact and consequences. There is no longer time to anticipate impacts of information technology before they become part of our everyday life, The pocket calculator and the citizen-band radio are cases in point.

I am a lawyer. I am not a telecommunications expert, nor do I pretend to understand the technology of computers. But one does not have to understand how the technology works to perceive its impact on society, including international society. Let us be blunt. The developments of instantaneous telecommunications and computer technology, linked together, have taken most of our countries (and their legal systems) by surprise. Suddenly, technological developments occurred which affected the place at which vital international information was stored. The jobs of citizens were affected. Unless proper safeguards were introduced, personal information on individuals in one country could be stored quite simply in another country, retrievable without technical hindrance in an instant and at costs which are constantly reducing.

THE FIRST REACTION: LOCAL DATA LAWS

The first reaction of lawmakers to the new information technology was the development of a series of national laws designed to protect individual liberties and to assure the security of personal data. In Sweden, the Data Act 1973 established a Data Inspection Board with significant powers of superintendence over automated collections containing personal data. In the United States, the Privacy Act of 1974 established a code for the protection of privacy in data files, automated and otherwise, kept by federal governmental agencies. From these beginnings, there has proliferated a large number of laws and proposals for laws. In France, the Act on Data Processing, Data Files and Individual Liberties came into operation in 1978. In Australia, the Law Reform Commission, which I head, has been set the task of designing national privacy laws.

A table illustrates the stage reached in domestic legislation on this topic:

STATUS OF DATA PROTECTION LEGISLATION

| Country | National | Sub-National | Reports |
|---|---|---|---|
| Australia | | L | RP |
| Austria | L | | R |
| Belgium | P | | |
| Canada | L | L | R |
| Denmark | L | | R |
| Finland | | | RP |
| France | L | | R |
| Germany | L | L,P | R |
| Greece | | | |
| Iceland | | | RP |
| Ireland | | | |
| Italy | | | RP |
| Japan | | | RP |
| Luxembourg | L | | |
| Netherlands | P | | R |
| New Zealand | L | | |
| Norway | L | | R |
| Portugal | | | |
| Spain | P | | R |
| Sweden | L | | R |
| Switzerland | | L | RP |
| United Kingdom | | | R |
| United States | L,P | L,P | R |
| Yugoslavia | | | RP |

Source : Transnational Data Report

Code

L = Law Adopted
P = Legislation in Parliament
R = Government Report Prepared
RP = Government Report in Preparation

The technology of instantaneous communication and the potential to collect and store vast quantities of information outside a country (and, therefore, possibly beyond its legal jurisdiction) attracted piecemeal attention in the early

domestic legislation of Europe. For example, s.11 of the Swedish Act provides that trans-border flows of personal data out of Sweden may only take place with the permission of the Data Inspection Board. Section 7 of the Danish Private Registers Act and s. 20(3) of its Public Registers Act make like provisions. Section 24 of the French law also envisages authorisation or regulation of the transmission of personal data, subjected to automatic processing, between France and another country.

## THE SECOND REACTION: INTERNATIONAL DIMENSION

### Causes of the "Second Wave"

A number of considerations led to a "second wave" of international concern and to the involvement of international organisations, including the Organisation for Economic Co-operation and Development (O.E.C.D.). Amongst the chief considerations I would list:

* Pace of Tele-informatics: The potentiation of information technology and telecommunications. Put together, the computer and the satellite, the data bank and the telephone make a nonsense of distance. The realisation of this in so many quarters and the massive development of the use of this technology has left domestic lawmakers gasping. The process of lawmaking in most democracies is a slow one. It is done by laymen. The technologies move fast and are beyond the comprehension of most laymen. What can be understood is that information is moving about at ever-increasing speed and ever-diminishing cost, indifferent to international borders and, therefore, not readily susceptible to domestic laws.

* Fear of Artifical Barriers: Especially in the contiguous states of Europe but also in other developed communities as a consequence of telecommunications advances, a fear was expressed that slow-moving lawmakers, modelling their laws on legal

concepts of earlier times, would impose barriers on the new technology which would be artificial, difficult to police and enforce, inconvenient and counter-productive.

* Fear of Inconsistencies in Laws: Even more pressing was the realisation that, with common technology, gave inconveniences could arise if utterly different approaches were adopted in relation to data protection and data security. The "hardware" and "software" of computers would be affected, with possible consequences for design and costs, to say nothing of the effect on links between data bases in different countries. Such links have a great potential for good as any airline traveller will know.

* Fear of Misusing Privacy Laws: A further concern, particularly in an organisation with the objects of the O.E.C.D. was, naturally enough, that, in the name of protecting privacy some countries would develop laws, policies and practices that were in fact aimed at solving other perceived consequences of the new technology, e.g., the feared loss of national sovereignty, diminished cultural independence, linguistic autonomy, lost job opportunities, technological excellence and expertise and so on. In other words, it was feared in some quarters that specific barriers would be created, ostensively in the name of protecting individual liberties, but in truth aimed at ulterior objects which, however legitimate they were considered at home, were wrongly "dressed-up" as a privacy concern.

* Fear of Taxes on Flows: Finally, I would mention a consideration raised by Mr J.P. Chamoux, a Consultant to the O.E.C.D. He suggested that as trans-border data flows became a significant part of international trade in goods and services principally in the flow of non personal data they would also attract the attention of tax authorities. The need to bring some order into this potential development was called to attention.

The result of some or all of these considerations has been a series of international efforts designed to address the consequences, legal and economic, of the expansion in trans-border data flows. It is no disrespect to the efforts of the United Nations Organisation, U.N.E.S.C.O., the European Communities Commission, the European Parliament and the Nordic Council to suggest that the chief international efforts so far have been in the Council of Europe and the O.E.C.D. Fortunately, there has been close collaboration between the Committee of Experts of the Council of Europe and the Expert Group of the O.E.C.D. The overlap of member countries and of working personnel, the commonality of the technology and of the problems to be faced promoted a high degree of co-operation both within these two bodies and between them.

Special Features of the O.E.C.D. Project

Nonetheless, the O.E.C.D. exercise has certain special features:

1. Wide Membership: The membership of the O.E.C.D. is wider and more diverse than the membership of the Council of Europe. In addition to its European members, the O.E.C.D. includes the United States, Canada, Japan, Australia and New Zealand. Because of the special significance of North America in relation to data processing, the economic importance of Japan, the more intensive representation of distant and Anglophone countries and of the Common Law tradition, the O.E.C.D. project is at once more universal and more diverse.

2. Guidelines not Convention: Whereas the Council of Europe Committee has drafted a convention, the O.E.C.D. Expert Group's mandate limited it to the drafting of Guidelines for voluntary observation, education and instruction in members countries, without excluding the development of a binding convention at a later stage.

3. Automated and Manual Data: Whereas the Council of Europe's draft convention relates to automated data, the O.E.C.D. Expert Group's mandate is not so limited. Its Guidelines will extend beyond personal data which is automatically processed.

4. Economic Issues: Non-personal Data: The O.E.C.D. Expert Group has a dual mandate. Not only must it develop guidelines on the basic rules governing trans-border data flows and the protection of personal data. It must also investigate the legal and economic problems relating to trans-border flows of non-personal data, including the issue of taxing policy called to attention by Mr Chamoux. Work on this second issue has now begun.

Neither the Council of Europe draft convention nor the Guidelines prepared by the O.E.C.D. Expert Group have yet completed their passage through the formal machinery of the two organisations. In the case of the O.E.C.D., the Fifth Meeting of the Expert Group took place in Paris on 12-14 September 1979. The Explanatory Memorandum to accompany and elaborate the Guidelines was settled. Both documents will now be submitted for consideration, ultimately by the Council of the O.E.C.D. Because the final form of the Guidelines has not yet been approved (and is at present the subject of home consultations), it is not possible for me to relate in any detail the precise terms of the Guidelines. Still less is it for me, an Observer only, to reveal the contents of the Council of Europe draft. These inhibitions do not prevent a broad explanation of the Guidelines and their significant for member countries and for individual citizens.

## THE FIRST EFFORT : HARMONISING PRIVACY LAWS

### The Golden Rule: Right of Access

Despite the differences of language, culture and legal and institutional traditions, what is remarkable when one looks at domestic legislation on information privacy (and therefore at the international instruments designed to harmonise them) is the recurring nature of the principles laid down for data protection and data security.

The "golden rule" of national laws on this subject is the right of individual access to personal data about oneself. This principle is at the core of the O.E.C.D. Guidelines. If nothing else is achieved in domestic privacy protection and in international efforts to protect privacy in trans-border data flows, than agreement about this "right of access", such accord will, in itself, be a most significant legal development.

An individual should have a right to obtain from a person who has control over data confirmation of whether or not the data controller has personal data on him. He should be entitled, within a reasonable time and at a cost (if any) that is reasonable to have access to data relating to him, supplied in a form that is readily intelligible. He should be entitled to challenge that data and, pending the determination of that challenge according to law, to have the record annotated concerning his challenge. If his challenge is successful, he should have the right to have the data corrected, completed, amended, annotated or, if appropriate, erased.

This is the central principle. It is found in almost every instrument on information privacy so far developed. Under the United States Privacy Act 1974 for example each agency that maintains a system of records is obliged "upon request by an individual to give access to his record or to any information pertaining to him which is contained in the system". The Canadian Act notes amongst the entitlements of the individual that he is entitled to ascertain what records exist concerning him, the uses to which they are put and to examine "each such record". The French law in s.35 confers an entitlement "to obtain access to information concerning him". The German Federal Act in s.4 confers a similar right as do the Austrian, Swedish and Danish laws.

The machinery for enforcement differs. In the United States it is, by internal bureaucratic machinery or by a civil action for damages in the courts. In Canada, the machinery is complaint to the Privacy Commissioner, who has ombudsman functions. In Europe, provision is typically made for the complaint to a data protection authority. Though the machinery

differs, this common principle is the lynchpin of information privacy legislation in Western countries. It is therefore the central provision of international efforts to harmonise such laws. Projects such as those of the O.E.C.D. Expert Group have a special usefulness in countries, including my own, where no privacy laws have yet been enacted. The development of Guidelines which adopt, on the international level, the principle of access to personal information, will both promote this proper principle, important for individual liberties, and help avoid the development of different and inconsistent principles that could adversely impact the free flow of information.

Other Rules of Data Quality and Security

Apart from the central provision, there are other rules of data quality and data security that are spelt out in the O.E.C.D. Guidelines.These are also reflected in municipal law. Amongst the common rules are:

* The collection limitation principle: that rules should be laid down governing the amount and method of collecting personal data.
* The information quality principle: that information should be accurate, complete and up-to-date for the purposes for which it may be used.
* The purpose specification principle: that the purposes for which personal data are collected should be identified at the time of collection. The use made of the data should generally be limited to those purposes or others permitted by law or agreed to.
* The disclosure limitation principle: that personal data should not be disclosed or made available except by consent, common and routine practice or legal authority.
* The securities safeguards principle: that personal data should be protected by adequate security.
* The accountability principle: that there should be an identifiable person accountable in law for complying with the principles.

The final form of the O.E.C.D. Guidelines on the "basic rules" for the protection of privacy and individual liberties, the scope of their application and the exceptions from their provision will have to abide the decision of the Council. Each of the above principles is, however, reflected (in differing language and with different enforcement machinery) in most of the national laws already passed or now proposed. By clarifying the general principles and putting them forward to the international community as an agreed standard, a conceptual framework is provided against which laws already enacted or proposed can be tested. The universality of the technology involved and the general desirability of free and unimpeded flows of information between nations require that local laws for the protection of information privacy should cluster around commonly accepted principles. If we can get the "basic rules" agreed and reflected in municipal law, that will itself be a most significant contribution to diminishing undue barriers to the free flow of information between countries.

THE SECOND EFFORT : INTERNATIONAL CO-OPERATION

There remains the question of legitimate restrictions on the free flow of data between nations. Countries should, be encouraged to refrain from developing laws, policies and practices, ostensibly for the protection of privacy and individual liberties, but going beyond what is needed for those purposes. In other words, if national security or economic, cultural or technological protection are to be invoked, there should be no endeavour to disguise them behind machinery established nominally for protecting information privacy.

Because the free flow of information is generally considered to be for the benefit of mankind, countries should take into account the impact which their domestic processing and re-export of personal data might have upon avoidance of the laws of other countries. They should promote uninterrupted and secure trans-border flows of personal data and refrain from restricting such flows, except where recipient countries do not provide protection for information privacy, substantially in accordance with the "basic rules". The development of

information exchange, mutual assistance and agreed principles of Private International Law are all desirable ends requiring further effort by the international community.

The O.E.C.D. Guidelines do not foreclose the possible development of a convention at a later date to establish legally binding rules that will govern these matters. At this stage of municipal law development, they suggest a looser and more flexible regime for the guidance of local lawmakers and as a first step towards any future binding rules of international law.

CONCLUSIONS

What does all this mean for the individual citizen? The development of information technology provides challenges to society, particularly when that technology is married to the concurrent rapid advances in telecommunications.

In the past there was protection for individual privacy in the massive bulk and inefficiences of manual files. Nowadays the capacity of the computer to store information in ever-increasing quantity, at diminishing cost and to retrieve it, integrate it and preserve it removes some of the practical protections that previously existed. The very development of the technology makes us increasingly dependent upon it. Decisions about individuals' lives in the future will more and more be made on the basis of personal data held on file about them. The telecommunications dimension makes the place at which such information is stored in data banks, increasingly irrelevant. Information on Australian citizens may be stored in Texas. Information on Swedish citizens may be stored in France. In each case, by telecommunications, the data base may be interrogated and will instantaneously respond. In these circumstances, domestic law could be readily circumvented. At the very least, it may be difficult to know which domestic law applies, which standards are to be observed, what rules are to be followed and how the individual should go about asserting his rights to information privacy.

It is for that reason that international organisations, including the O.E.C.D., have begun the search for principles that will promote uniformity in domestic laws and co-operation at an international level. I do not pretend that the O.E.C.D. Guidelines will provide a complete and enforceable system, actionable at the behest of an aggrieved individual. They do not. But by spelling out the "basic rules" to be observed in home legislation to protect information privacy and individual liberties, they may contribute to harmonising municipal laws and to diminishing the discordancies that would otherwise arise from local experimentation in lawmaking. They will be especially useful in those member countries of the O.E.C.D. (about half) including Australia and Japan, in which no fully developed and enforceable privacy protection laws have yet been enacted.

The law is an instrument for stating and ultimately enforcing society's standards. It is important, even at a time of fast-moving technology, that the law should continue to assert and uphold the rights of the individual. The Rule of Law is the banner of the Western communities. Information science brings in its train great opportunities for mankind. But it also brings challenges, amongst other things, to individual human rights. The business of the O.E.C.D. Guidelines is to suggest at the international level what information privacy laws seek to attain in the national scene. This is the maintenance of the proper balance between the general free flow of information within and between nations, on the one hand, and upholding individual privacy and human liberties, on the other. It is a heartening to find that concensus can be reached on principles of national and international application. Across the world and bridging many different cultures, an important agreement has been struck which will, I hope, make a contribution to defending the individual in a time of great technological change.