MADRID CONFERENCE ON THE LAW OF THE WORLD

TUESDAY, 18 SEPTEMBER 1979

O.E.C.D. GUIDELINES ON PRIVACY

Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission

October 1979

MADRID CONFERENCE ON THE LAW OF THE WORLD

TUESDAY, 18 SEPTEMBER 1979

O.E.C.D. GUIDELINES ON PRIVACY

Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission

PROTECTING MODERN INFORMATION PRIVACY

Mine is an address on the international dimension of protecting privacy in the age of computers, satellites and telecommunications. In Australia the right to privacy is protected by "piecemeal and unco-ordinated" laws that are inadequate for the challenges to privacy that is important in today's world: namely, the right to privacy of personal information files especially in computers. This right has become called in Europe (perhaps more accurately) "data protection" and "data security". Nowadays, privacy is invaded much more through files than through keyholes.

Because of the inadequacy of legal protections in Australia, the Australian Government asked the national Law Reform Commission which I head, to develop and propose to the Australian Parliament new laws that would guard individual privacy in the computer and telecommunications age. Work towards our report on this subject is well advanced. It is expected that there will be national legislation on this subject before 1984.

PROLIFERATING DATA LAWS

Over the past decade many countries have developed new laws on this subject. Starting with the Hesse Law of 1970 and the Swedish Data Act in 1973, there quickly followed many laws to protect the privacy of personal information files, especially in Europe and North America. The proliferation of such laws, in turn, led to concern that differing legal standards and machinery - impacting a basically common technology (especially computers talking to each other in different countries) - might impede the rapid flows of personal information which are generally thought to be for the benefit of mankind. Most of us would not be here but for the instantaneous flows of data about us through the airline computers. The necessity to get official authorisation for such flows every time they occurred could bring the flows to a sudden halt.

INTERNATIONAL HARMONISATION

It was the realisation of that danger and fears of the misuse of "so called privacy legislation for other, different national purposes (job protection, defence of culture, language and sovereignty) that led to the establishment of a number of international inquiries into privacy laws. These inquiries have been proceeding in the context of such bodies as:

- The United Nations Organisation
- U.N.E.S.C.O.
- The European Parliament
- The Commission of the European Communities
- Nordic Council

but most actively

- The Council of Europe
- The Organisation for Economic Co-operation and Development (O.E.C.D.). This body consists of Western European countries, Yugoslavia, the United States, Canada, Japan, Australia and New Zealand.

The Council of Europe is drafting a convention. The O.E.C.D. was asked to draw up guidelines on the basic rules for privacy protection. By getting an agreed statement on the basic

principles that could be reflected in national law - it was hoped that disparities that would unnecessarily impede international flows of data could be avoided.

I was elected Chairman of this O.E.C.D. project. The fifth meeting on the subject took place in Paris this month, so this report on the development of international principles is "hot off the press". Because the final guidelines are now being considered by home governments and in the Council of the O.E.C.D., I can only sketch them in general terms. When approved and published they will, I believe, provide a useful intercontinental framework for modern laws on privacy where it matters most: defending the individual against the perils of computerised information. No country will be immune from this issue.

A "GOLDEN THREAD": THE RIGHT OF ACCESS

Despite difference of language, culture and legal traditions, what is remarkable when one looks at domestic laws on information privacy is the recurring nature of the principles laid down. 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 and Council of Europe draft convention. 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 federal governmental agency which 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 countries that have enacted it. 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 around the world.

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 those dealing with:

1. The collection limitation principle: that rules should be laid down governing the amount and method of collecting personal data.
2. The information quality principle: that information should be accurate, complete and up-to-date for the purposes for which it may be used.
3. 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.
4. The disclosure limitation principle: that personal data should not be disclosed or made available except by consent, common and routine practice or legal authority.
5. The security safeguards principle: that personal data should be protected by adequate security.
6. The accountability principle: that there should be an identifiable person accountable in law for complying with the principles.

These principles are 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 a benchmark, 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 amongst all of our countries.

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 inevitable inefficiencies of manual files. Nowadays the capacity of the computer to store information in ever-increasing quantity, at diminishing cost and increasing speed 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 French citizens may be stored in the United Kingdom. In each case, by telecommunications, the data base may be interrogated and will instantaneously respond. In these circumstances, domestic laws 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 in data banks abroad.

It is for these reasons that international organisations 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 our form of society. 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. What I have been talking about 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 heartening to find that general consensus can be reached on principles of national and international application. Bridging many different legal cultures, an important agreement is proposed which will, I hope, make a contribution to defending the individual in respect of great technological changes. It is not an exaggeration, in a time of big business, big government and big technology, to declare that for "information privacy" you should read "individual freedom".

Il me faut vous avouer que j'ai tout particulierement apprecie l'occasion qui m'a ete donne de me trouver parmi vous au cours de cette semaine. C'est le meilleur des souvenirs que j'en reporterai dans mon pays.