STANFORD LAW SCHOOL

STANFORD JOURNAL OF INTERNATIONAL STUDIES

MAY, 1980

TRANS BORDER DATA FLOWS & THE "BASIC RULES" OF DATA PRIVACY

The Honourable Mr. Justice M.D. Kirby

January 1980

TABLE OF CONTENTS

STANFORD LAW SCHOOL

STANFORD JOURNAL OF INTERNATIONAL STUDIES

MAY, 1980

TRANS BORDER DATA FLOWS & THE "BASIC RULES" OF DATA PRIVACY

The Honourable Mr. Justice M.D. Kirby*

PROLIFERATION OF PRIVACY LAWS

On the eve of the 1980s, the influential London Economist indulged in new decade futurology speculation. Amongst its prognostications was the suggestion that the scope for advances in telecommunications would be "aborted in bureaucracies' or price controllers' grip". Privacy regulations, it predicted, would impede data processing without actually safeguarding privacy.[1]

The close of the 70s saw an energetic effort in a number of international organisations addressed at the proliferation of data protection (privacy) laws. Central to this international endeavour has been the attempt to define certain "basic rules" which can be used as a benchmark for privacy legislation. There is no doubt that the expansion of automated processing of personal and other data has greatly benefited mankind. But there is equally no doubt that lawmakers and those who advise them, in the developed world at least, perceive certain dangers to the individual, which require protective legislation. This perception has led to specific data protection laws in the United States, Canada and Western Europe. In many other countries, including Australia, inquiries are well advanced

towards the design and adoption of privacy protection laws. In some of the legislation already passed, specific provisions are enacted by which a local data protection authority may control the trans border flow of personal data either by a licensing provisions as in the case of Sweden and Denmark[2] or by a system of prior authorisations, as in the French law.[3] Typically, the justification offered for such provisions is that the instantaneous nature of new information technology facilitates the ready haemorrhaging of personal data unless international as well as local purveyors of information can be readily controlled. There would be little point in erecting protective legislation in one country if the protections could be readily circumvented by the inexpensive expedient of storing data across the border where it was beyond the jurisdictional control of privacy laws, yet could be readily and cheaply retrieved via international telecommunications systems which were themselves protected from scrutiny by the rubric of secrecy.

Put positively, there has been a concern that unintended disparities in the laws of friendly countries could create unexpected adverse effects on the general free flow of data between countries. It being considered that trans border flows of data (including personal data) contribute to economic and social development, the removal of unintended or unexpected impediments arising from differing regulatory machinery has been a chief effort of the international moves towards harmonisation. The adoption at an international level of agreed principles might help to promote harmonisation or standardisation of laws, which could otherwise develop in a discordant and inconsistent fashion, thereby creating the ineffective bureaucratic impediment to growth and development feared by the Economist.

Put negatively, the fear has been expressed in some quarters that, in the name of privacy protection, legislation might be developed which could actually have other national purposes in mind. Put bluntly, this is the fear of "data protectionism". Legislation, nominally for the purpose of data protection, could actually have such objects as the protection of domestic employment, local technology and expertise, home

industries, national culture, language, sovereignty etc. Accordingly, it has been suggested that there would be merit in an international definition of the general rules against which legislation, ostensibly for the protection of privacy, could be publicly measured. Such an international standard might reduce or discourage the adoption of illicit national legislation which imposed an artificial barrier on the general free flow of information, including personal information.

This is the background to the search for the "basic rules" of privacy protection laws. Given the different languages, different legal traditions and differing cultural and social values, it might have been expected that such a search would have been frustrated by fundamental disagreements. The fact is that in all of the major international efforts that have so far addressed this problem, there has been a broad measure of agreement on the "basic rules" around which domestic privacy legislation should cluster. In a statement made by me to the Committee for Scientific and Technological Policy (C.S.T.P.) of the Organisation for Economic Co-operation and Development (O.E.C.D.) I reported a broad consensus in an O.E.C.D study addressed to this issue :

> At the heart of the basic rules is a simple idea. It is the so-called "golden rule" of the protection of privacy and individual liberties. This is the right of the individual, in general, and with some exceptions specifically provided for, to have access to personal data about himself. If this rule is accepted, not only will the individual know the ways in which he is perceived by others. He will, by inference, have power to amend and correct personal information which is untrue, unfair or otherwise lacking in appropriate quality. In addition to this fundamental rule, a number of other basic rules were identified. These relate to the "input", "throughput" and "output" of personal information. They govern the rules that should control the collection, use and security of personal data.[4]

The speed with which countries linked to each other by rapidly expanding ties of data traffic are developing privacy and data protection laws make it imperative that the "basic rules" should be identified as quickly as possible. Otherwise the opportunity might be lost to influence the lawmaking process in those countries which have not yet developed privacy protection

machinery. The inefficient bureaucratic nightmare, imposing cumbersome, ineffective and expensive impediments to international data traffic, could still develop. There will be less chance of this happening if data protection and data security laws continue to follow a basic scheme identified in an international instrument. At a later stage, international treaties may be necessary to go beyond international self-regulation and to provide effective machinery for the enforcement of the "basic rules" in one country, by a resident of another. But unless the "basic rules" can be promptly identified, an opportunity may be lost to influence the development of legislation in countries such as Australia, Japan, the Netherlands and the United Kingdom, where privacy laws are planned but have not yet been enacted.

PRIVACY PROTECTION IN AUSTRALIA

Absence of General Legal Protection. Australia has a Federal Constitution which was modelled on that of the United States. Limited powers are conferred on the federal (Commonwealth) Parliament to make laws for the whole of the country. If not conferred on the Commonwealth Parliament, lawmaking powers remain with the States.[5] There is no general Bill of Rights nor is there any explicit mention of a right to privacy in the Constitution. The observance of respect for individual privacy is secured without much support from legislative sanctions. Partly as a reaction to technological developments, steps are now being taken to supplement rudimentary common law protections afforded by the inherited common law of England (trespass, assault etc.) As there is no general power in the Commonwealth Parliament to make binding laws for the protection of privacy throughout Australia, that protection remains, substantially, a State matter, except in specific areas of federal responsibility.

The common law of England, and its variant in Australia, did not develop any general legal principles for the protection of individual privacy. Although this is curious, given the importance which Anglophone people generally attach to the cultural value of privacy, it remains a fact of legal life. In 1937 an attempt was made to persuade the High Court of Australia (the federal Supreme Court) that a right to privacy

existed in the common law of Australia. In the result, however, the court rejected the contention. The Chief Justice of the time said :

> However desirable some limitation upon the invasions of privacy might be, no authority was cited which showed that any general right of privacy exists.[6]

In view of this decision, if general or specific protections for privacy are to be developed in the law of Australia, they will probably have to be developed either by the legislative or executive arms of government. Innovative developments by the courts cannot be anticipated.

The federal area of responsibility includes a number of concerns that are relevant to significant privacy protection. They include the federal Public Service and the Australian Territories (the Capital and Northern Territories, Antarctica and certain Island Territories) where there is plenary federal power. Other areas of relevant power include interstate trade and commerce, telecommunications, census and statistics, banking and insurance.

In only one Australian State, New South Wales, is there general legislation on privacy protection. A Privacy Committee has been established in that State with general powers of conciliation, investigation and advice but without enforceable sanctions.[7] There is no Australian legislation, Federal or State, specific to information systems generally or automatically processed data systems in particular. Legislation exists which affects privacy protection indirectly. Furthermore codes of conduct have been developed by the Australian Computer Society, the N.S.W. Privacy Committee, the Australian Public Service and individual owners and operators of information systems. The rapid advances of technology have outstripped legal protections for privacy and individual liberties. The realisation of this has led to a significant effort, Federal and State, to develop effective legislation.

At a federal level, the Australian Law Reform Commission has been given the task of developing and proposing laws for the protection of privacy in the federal sphere. The Commission is a permanent statutory authority which receives references

from the federal Attorney-General, develops proposals by procedures of public consultation, and finally produces a report which is tabled in Parliament. Typically, reports attach draft legislation. The Commission was established in 1975 and its reports on several topics have been followed by legislation at both a State and Federal level in Australia.[8] The Commission's work on its privacy reference is proceeding in close consultation with State inquiries and with the international efforts addressed at defining the "basic rules" which should be reflected in domestic privacy law.

The State inquiries in Australia need not be described at length. In New South Wales, the Privacy Committee has produced an "exposure draft" suggesting basic rules for privacy in information systems for adoption on a voluntary basis by record-keepers throughout the State.[9] In Victoria a committee of the Parliament, the Statute Law Revision Committee, has received a reference to inquire into privacy generally. In Queensland the local law reform commission has been requested to consider the protection of privacy. In South Australia a departmental committee has been examining privacy protection. A new State Government has recently undertaken to consider legislation following the report of the Australian Law Reform Commission. In Western Australia a reference has been given to the local law reform commission in terms parallel to that of the federal commission. In Tasmania a Parliamentary Committee has been examining a Privacy Bill designed to create a general statutory tort of privacy. If it is important to develop privacy laws which are compatible as between the members of the international community, it is even more important that within the one federal country, privacy protection laws should be compatible so that inefficiencies and evasion can be reduced and mutually protective assistance facilitated.

Scattered, piecemeal Privacy Protection. Despite the absence of a general right to privacy either in the common or statute law of Australia, specific legislation provides protection for particular aspects of privacy. A number of Acts of the Federal Parliament, for example, require the observance of confidentiality by officers of the federal Public

Service.[10] Responsibility for telecommunications is a federal matter. The privacy of the mail and telegraphic, telephone and other like services in Australia is secured by tradition, supported by specific legal obligations. The Telephonic Communications (Interception) Act, 1960, for example, forbids any person from intercepting, or authorising or permitting another person to interfere with communications passing over the telephone system. Only two exceptions are allowed, namely for service or maintenance and in pursuance of a legal warrant. The latter are cases limited to national security and, since recent legislation, certain cases involving narcotic drugs.[11]

In addition to the federal legislation, a number of State Acts have been passed to protect privacy on a piecemeal basis. In five of the States, the use of listening devices is controlled by legislation limiting the cases in which such devices may be used to hear, record or listen to a private conversation. The sanctions include criminal penalties and provisions forbidding the reception into evidence of details of any such private conversation unless obtained following appropriate judicial or ministerial authorisation. The only other major area of State legislation for the protection of information privacy in Australia relates to the activities of credit reporting agencies. It has been estimated that credit reports are kept on about three million people in Australia, a country with a population of fourteen million. In New South Wales, credit bureaux have entered into a voluntary agreement initiated by the State Privacy Committee. This facilitates consumer checking of credit records. A similar agreement has been implemented in the Australian Capital Territory. In Queensland, South Australia and Victoria certain operations of credit reporting agencies are regulated by statute.[13] These Acts provide a means of access by consumers to records kept about them by a credit reporting agency. They provide machinery for correction of disputed information and for notification to be given to traders to whom the incorrect information had been supplied. In addition to such piecemeal legislation as has just been described, State and Territory criminal law provides sanctions, either by legislation or by common law, for such invasions of privacy as assault, trespass,

entry on to property without permission and so on. Many of these criminal sanctions are paralleled by civil law entitlements to sue for damages in tort.

A number of proposed federal laws should also be mentioned. In 1977, the Federal Government introduced a Criminal Investigation Bill designed to regulate, for the first time in a comprehensive statute, the criminal investigation activities of Federal Police in Australia. The Bill is based substantially on a report of the Australian Law Reform Commission.[14] The Bill lays down requirements with respect to police procedures of arrest, search, interrogation, the recording of interviews, medical examinations and so on. Provision is made for sound recording of confessional evidence to police and for destruction of such recordings in certain circumstances. Specific provision is also made with respect to police records. Clause 67 of the Bill requires the Police Commissioner to "take and cause to be taken such reasonable measures as are necessary to ensure the accuracy and security of the records of the ... police force". Prohibitions, supported by criminal penalties of fine and imprisonment, are contained in relation to copying, extracting or communicating of information in police records. In certain circumstances, upon the payment of a prescribed fee, information from police records can be given to the person involved. The Bill lapsed with the dissolution of the Australian Parliament in 1977. However, it is expected that it will be reintroduced in 1980.

In 1978 a Freedom of Information Bill was introduced to provide a prima facie right of access by the individual to government information. The Bill provides for certain exceptions to the provision of access to government information, including where disclosure would amount to an unreasonable disclosure of the personal affairs of an individual affected thereby. Disputes concerning exemptions are, for the most part, capable of being resolved by the Administrative Appeals Tribunal. The Bill is still before the Australian Parliament and has recently been the subject of a report by a Senate Committee which criticises the scope of certain of the exemptions from the right of access.[15]

Finally, in 1979 the Government introduced a Human Rights Commission Bill to establish a Human Rights Commission. The Bill envisages, amongst other things, that the Commission will report to the Federal Parliament on the observance by federal laws of the standard contained in the International Covenant on Civil and Political Rights. The Covenant is a schedule to the Bill. Although Australia has signed the Covenant, it has not yet ratified it. Nevertheless, there is a commitment by successive governments to ratify the covenant and ratification is expected in 1980. The covenant includes in Article 17 the following provisions :

17.1 No-one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

.2 Everyone has the right to the protection of the law against such interference or attacks.

The Human Rights Commission Bill envisages Ombudsman-like machinery for sanction by way of report to Parliament. Such reports will call attention to the provisions of the law that are incompatible with the covenant, or inadequate to effect its obligations.

Law Reform Reports. It is against this background of piecemeal, scattered, inadequate legal protection that the Australian Law Reform Commission addresses the task of suggesting privacy legislation in Australia. Although limited to the federal sphere, it is likely that developed proposals on privacy protection put forward by the Commission will also significantly influence State privacy laws. The possibility of this happening has been enhanced by close co-operation between State and Federal inquiries. It has also been encouraged by the involvement of Australia in the O.E.C.D. exercise, described below. As the O.E.C.D. guidelines were developed, a series of national seminars were conducted, in which representatives of State privacy inquiries, business and commercial interests, Federal Government Departments and academics took part. The result has been the focusing of national attention in Australia upon the "basic rules" of privacy protection as these "basic rules" have been refined and developed at an international level.

So far, the Australian Law Reform Commission has produced two reports, in partial discharge of the reference on privacy protection. The first, Unfair Publication : Defamation and Privacy[16] proposed the development of certain new laws for the protection of privacy in the context of the publication of defined "private facts". The report proffered draft legislation for a uniform or national defamation law in Australia. At a time when information is published substantially nationally (whether by electronic or printed means) the proliferation of defamation laws can result in undue caution, as editors seek to comply with the lowest common denominator. Influenced by the experience of the United States and developments in Canada and Europe, the Commission proposed the development of a new legal concept of "unfair publication". This actionable wrong was defined to include :

(a) a publication of defamatory matter concerning a person;
(b) a publication of sensitive private facts concerning an individual; or
(c) an appropriation of the name, identity, reputation or likeness of a person.[17]

Defences were provided for, including consent, authority of law, privilege and that the publication was relevant to a topic of public interest. It is apt to mention that in Australian law there is no provision equivalent to the First Amendment of the United States Constitution.

The report on unfair publication is now before the Standing Committee of Federal and State Attorneys-General with a view to the adoption of a uniform Act in Australia. The treatment of privacy protection in publications was dealt with as a separate issue in Australia because of the concurrent inquiry into defamation law reform and because one of the impediments to uniform defamation laws was the existence, in some jurisdictions of Australia, of a requirement that to justify a publication, the defendant had to show not only that it was true, but that it was published "for the public benefit" or "in the public interest". The existence of these defences constituted a limited protection to privacy and their abolition required any new defamation law to address this special facet of legal protection for privacy and to provide an effective

substitute. The substitute proposed was a new statutory tort embracing defined protection against the publication of private information.

The report of the Law Reform Commission on Privacy and the Census[18] is more germane to the present discussion. It represents the first report on an aspect of information privacy. The subject was dealt with separately and in advance of the general topic because of a request of the Federal Attorney-General that specific attention be given to the implications for individual privacy of the national Australian Census, in view of a controversy on the subject which accompanied the last census in 1976. The intention to conduct the next Census in 1981 caused the Federal Treasurer to request that the Commission deal with the topic in advance of its general report on privacy protection in the federal sphere. The census is the one universal, national and compulsory collection of personal information which takes place in Australia. Accordingly, the principles that should govern the collection, storage and use of personal information for census and statistical purposes posed a special but important species of the problem of balancing the utility of information and the protection of privacy.

The report suggests the adoption of certain principles for the protection of privacy interests. These include the principle that personal information should only be collected if it is necessary for achieving the specific aims of the collection,[19] that an individual should be properly informed in relation to the nature and purposes of the collection from him of personal information,[20] that highly sensitive personal information should not be sought, particularly on a compulsory basis, unless there are compelling reasons for collecting it,[21] that strict procedures should be adopted that avoid unwarranted disclosure of personal information to third parties,[22] that personal information which has been collected for a purpose should not normally be disclosed without consent for other purposes[23] and that as a general principle an individual should normally be allowed to have access to and to challenge a record of personal information about himself.[24] The particular applications of the general rules need not

detain us here. It is sufficient to mention the specific reference made to information privacy legislation developed in Europe and North America[24] and to the principles identified by international organisations such as the Council of Europe and the O.E.C.D.[26]

The Australian Law Reform Commission will, in 1980, publish two discussion papers dealing with the balance of its privacy reference. The first will address certain problems of federal regulation of privacy invasive intrusions (entry by federal officers, use of surveillance devices, telephone tapping etc). The second will deal with information privacy generally as it falls under federal regulation. The discussion papers will then, in accordance with the procedures of the Commission, be the subject of an exhaustive series of public hearings and seminars as well as direct private consultation with the bodies most immediately affected. It is hoped that a report will be produced, with draft legislation, by the end of 1980 or early in 1981. The discussion paper on the protection of privacy in personal information systems will draw specifically on the "basic rules" identified in the efforts, national and international, that have gone before : seeking to crystallize the principles which legislation on data privacy should observe. I now turn to an examination of the efforts to define the "basic rules" and an illustration, from laws already passed, of the implementation of the "basic rules" in national privacy legislation.

THE SEARCH FOR THE "BASIC RULES"

United States. It is not typical of the development of legislation in countries of the common law tradition for there to be clear articulation of principle before legislation is proposed for enactment. Our highly specific and detailed mode of drafting legislation, our traditions of judicial interpretation of legislation and the sheer pressure of business of Congress and Parliaments, as well as the inclinations and expertise of legislators, dampen the enthusiasms of the conceptualist. Of course, lawmakers and legislative draftsmen have certain fundamental principles in mind. But it is not typical for these to be flushed out and defined and then included, in terms, in statutory provisions.

The report of the United States Privacy Protection Study Commission put it thus :

> The requirements of an act, although not always easy to interpret, derive from the words of legislation. Principles, on the other hand, are sometimes less readily apparent. The statement of principles in a law's preamble, the law's legislative history, and the conditions of problems that led to its passage must all be read along with the language of its specific provisions. Although many issues in the 1960s and early 1970s were loosely grouped under the category of invasions of privacy, it is clear that many of the perceived problems had very little in common. ... The inquiry into these matters by a number of congressional committees did not share a common analytical framework, nor were the distinctions among different types of privacy invasions sharply drawn.[27]

The search for an "analytical framework" for privacy protection laws in the United States received an impetus when, in 1972, the Secretary of Health, Education and Welfare, Mr. Richardson, appointed an advisory committee on automated personal data systems. The committee's terms of reference were limited to the impact of computers on record-keeping about individuals specifically in the social security sphere. After grappling with the unsatisfactory problem of the definition of privacy, the committee concluded that it was the ability of the individual to have some control over the use of records about himself which constituted the most significant relevant aspect of the way organisations kept personal information. Five principles were propounded as a "code of fair information practices" designed to guide the striking of a fair balance between the legitimate requirements of the information gatherer, on the one hand, and the prerogatives of the individual, on the other. In tracing the development of the "basic rules" of information privacy, it is helpful to record these five principles :

(1) There must be no personal data record-keeping systems whose very existence is secret.

(2) There must be a way for an individual to find out what information about him is in a record and how it is used.

(3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

(4) There must be a way for an individual to correct or amend a record of identifiable information about him.

(5) Any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[28]

These five principles of fair information practices plainly influenced the form of the United States Privacy Act of 1974. However, in developing that Act, the Congress, guided by its own inquiries, developed the five principles further. According to the Privacy Protection Study Committee, eight principles can be discerned in the 1974 Act. Because of the importance which the Commission's presentation of these eight principles has had in the development of international guidelines, it is useful to set them out in full :

(1) There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices and systems. (The Openness Principle).

(2) An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information. (The Individual Access Principle).

(3) An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information. (The Individual Participation Principle).

(4) There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information. (The Collection Limitation Principle).

(5) There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation

(6) There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosure Limitation Principle).

(7) A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate. (The Information Management Principle).

(8) A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle).[29]

So far as principles were concerned, the Privacy Protection Study Commission urged that any clarification of the Privacy Act should incorporate "reasonableness" tests to allow flexibility and to give record-keeping agencies incentives to attend to implementation and to take account of differences between manual and automated record-keeping.[30] No fundamentally different or new basic principles were proposed, although many and varied suggestions were made concerning amendments to the Privacy Act and supplementary legislation.

Council of Europe. Three data protection laws were in operation in Europe when the United States Privacy Act of 1974 came into force. These were the national legislation of Sweden and two State laws of the German Länder, namely Hesse and Rhineland-Palatinate. The Hessian Act[31] was a "pioneer venture"[32] in that it was the first separate law laying down rules of general application for data protection, not specifically contained in legislation establishing a data centre. It was limited to computerised data in the public sector. It contained rules for conduct of computer personnel and the rights of individuals about whom information was stored. Protective machinery, including a Data Protection Commissioner, was established. The model was later followed in other Lander.

The Swedish Data Act was the first national law. It established a comprehensive set of rules concerning data processing by private as well as public users. A Data Inspection Board was established and other remedies and sanctions were instituted. The Swedish legislation set the stage for many subsequent European laws. Variants have already been enacted in Denmark, France, Norway and Luxembourg. In Germany and Austria an alternative model has been developed which does not require the registration of data banks but establishes a data protection authority to monitor a system which depends, significantly, on self-regulation. In Canada in 1977, a Privacy Commissioner was established as a member of the national Human Rights Commission. Canadian citizens and permanent residents have been given certain rights with respect to the handling of personal information held by the Federal Government. The Canadian model has been followed, in part, in New Zealand. The national Human Rights Commission of that country has been given the obligation to develop proposals on privacy protection. In addition, legislation establishing a national computerised government information system for the Departments of Police and Justice and the Ministry of Transport includes detailed measures for protection of privacy. A Privacy Commissioner is created and rights of indirect access and correction are assured, specific to the Computer Centre at Wanganui.[33]

The contemporaneous development of data protection laws at a national and provincial level in Europe, and the planned enactment of laws in other European countries, initiated a number of projects designed to secure harmonisation and compatability among those laws. The nature of information technology and the geographical proximity of the nations of Europe, as well as shared cultural, political, telecommunications and trade interests, made the effort to secure harmony in legislation natural and indeed inevitable.

As early as January 1968 the Consultative Assembly of the Council of Europe adopted a recommendation seeking a study of the effectiveness of the protection offered by the European Human Rights Convention against violations by modern scientific and technical devices of the right of individual privacy.

Following a number of reports, a Committee of Experts was established in 1971 specifically to address the protection of privacy in respect of the use of computers. As a result of the reports of that committee, two seminal resolutions were adopted by the Committee of Ministers of the Council of Europe. The first, adopted in September 1973, annexed certain principles applying to personal information stored in electronic data banks in the private sector. The second, adopted in September 1974, annexed like principles in relation to the public sector.[34] As Dr. Hondius has explained, although for operational reasons two separate resolutions were adopted, the guiding idea was that fundamentally the same rules should apply in both spheres. In 1974 it was considered that the time was not yet ripe for a European Convention because electronic data processing (the subject matter of the resolutions) was still in an initial phase. The enactment of legislation in the late 1970s in a number of European countries and the developing sense of urgency to resolve the interjurisdictional problems raised thereby led to the formation of a new committee of experts on data protection with the specific tasks assigned to prepare for consideration a draft Convention for the protection of individuals with regard to automated data files. That committee has substantially concluded its work on the preparation of a draft Convention. Initially the proposed Convention was intended to cover the member countries of the Council of Europe only. However, when in July 1977 the Committee of Experts received a formal mandate to prepare a draft international Convention, the scope was broadened to contemplate possible adherence by other non European countries.

Chapter II of the draft Convention is that which contains what are described as the "basic principles for data protection". The influence of the resolutions of 1973 and 1974 can clearly be seen in the language used. Article 4 imposes a duty on contracting parties to take the necessary measures in domestic legislation to give effect to the basic principles. Article 5 sets out requirements concerning the quality of personal data which is to be automatically processed. Article 6 contains special provisions in relation to certain defined categories of sensitive data. Article 7 requires appropriate

measures to be taken for data security. Article 8 contains additional safeguards for the data subject, enabling the individual to secure data protection for himself. Article 9 provides limitations on the exceptions and restriction of the exercise of the rights previously mentioned. Article 10 imposes on countries the obligation to establish appropriate sanctions and remedies for violations of domestic data protection law and Article 11 saves domestic legislation conferring a wider measure of protection on data subjects.

Although a draft Convention in final form was adopted by the Committee of Experts at its fourth meeting in Strasbourg in May 1979, at the end of the 1979 negotiations were continuing concerning certain provisions of the proposed Convention. These would not, however, appear to affect the "basic principles" which are less a matter of controversy than other provisions.

European Communities. The European interest in data regulation has been paralleled in the institutions of the European Communities. In November 1973 the E.E.C. Commission delivered a report to the Council for a Community Policy on Data Processing.[35] The focus of this communication was more upon the need to develop European industry than to protect individual liberties, including privacy. Nevertheless, the report concluded that the creation of data banks joined increasingly by international links would oblige the Community to establish common measures for the protection of its citizens.

Early in 1975, following a report of the Legal Affairs Committee, the European Parliament adopted a resolution in which it expressed its conviction that a Directive on individual freedom and data processing should be prepared urgentlyimposing on Community members the obligation to provide maximum protection to citizens against abuses or failures of data processing procedures and at the same time to avoid the development of conflicting national legislation. In 1976 the European Parliament adopted a resolution which instructed the Legal Affairs Committee to draw up a further report on the subject. Mr. Bayerl was appointed rapporteur. The

sub-committee was formally constituted in 1977 and public hearings of experts were held in 1978 and 1979. A report containing a motion for a resolution was presented in May 1979 and adopted in the dying hours of the last European Parliament based by the Bayerl report[36]. The resolution contains a recommendation from the European Parliament to the E.E.C. Commission and Council concerning the "principles" which should form the basis of community norms on the protection of the rights of the individual in the face of developing technical progress in the field of data processing.[37] The Recommendations are divided into three parts. Part I contains, amongst other things, what have been called the "basic rules". However, the first recommendation is that computerised or manual personal data banks should be subject to prior registration or authorisation by a data protection body. Part II deals with the rights of individuals to assert and uphold the basic rules. Part III envisages the appointment of an independent Community body as the "data control body of the European Community".

No action has so far been taken on the resolution of the European Parliament. The formal position is that the Commission of the European Communities is awaiting the completion of the draft Convention of the Council of Europe. The Commission has been represented as an observer in the work of the Council of Europe Committee of Experts.

O.E.C.D. It is in the Organisation for Economic Co-operation and Development that the United States, Australia and other non European countries are afforded the opportunity of influencing most directly the international specification of the "basic rules" for privacy protection legislation. The O.E.C.D. comprises 19 countries of Europe, the United States, Canada, Japan, Australia and New Zealand. Yugoslavia has a special associated status. Concern about the social implications of computer development was expressed in the O.E.C.D. as early as 1969. Specific concern about the policy issues for trans border data flows following the introduction of privacy protection legislation has been evident since 1970. In 1971 a consultant's report was secured on "Digital

Information and the Privacy Problem".[38] In June 1974 the O.E.C.D. organised a seminar on "Policy Issues in Data Protection and Privacy".[39] Among the issues considered were the problems that might arise as a result of the enforcement of domestic privacy laws in trans border data flows. Between 1974 and 1977 the Data Bank Panel analysed and studied a number of aspects of the privacy issues which sought to identify, within the context of the Organisation, basic rules on data protection and data security. The Data Bank Panel organised a symposium in Vienna in 1977. Following this symposium, it was decided to terminate the activities of the Panel and to create a new intergovernmental Expert Group on Trans Border Data Barriers and the Protection of Privacy. This Group was formally established in February 1978 by the Committee for Scientific and Technological Policy. The terms of reference of the Expert Group required it to :

(i) develop guidelines on basic rules governing the trans border 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;

(ii) investigate the legal and economic problems relating to the trans border 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 was instructed to carry out its activities in "close co-operation and consultation" with the Council of Europe and the European Community and to complete its work on item (i) by 1 July 1979. I was elected Chairman of the Group at its first meeting in April 1978. Although some work has been done on item (ii), the fast proliferating legislation, the currency of national inquiries on future legislation and the deadline imposed by the mandate all dictated that priority of attention should be given to developing the guidelines on the "basic rules".

The Expert Group met on six occasions and the results of its labours were presented by me to the Committee for Scientific and Technological Policy of the O.E.C.D. on 21 November 1979. In accordance with its instructions, the Expert Group at its fourth meeting in May 1979 agreed to the draft Guidelines, within the time specified. These were transmitted for approval and work continued on an Explanatory Memorandum to accompany and clarify the Guidelines. At a fifth meeting of the Expert Group in September 1979 the Explanatory Memorandum was also completed. However, when these documents were circulated certain suggested amendments and reservations were proposed. It was in the hope of removing these that a sixth meeting was called in November 1979 to coincide with the meeting of the Committee for Scientific and Technological Policy. In the result, most of the outstanding amendments and reservations were satisfactorily dealt with by the experts but five remained outstanding. Only one of these affects the "basic rules" on privacy protection. Most, if not all, represent questions for resolution at a political, not an expert, level.

At the time of writing (January 1980) the Guidelines have not been adopted by the O.E.C.D. Council. In accordance with the rules of the Organisation, they are therefore restricted in their circulation. Most of the controversies centre around provisions relating to the international flow of data. The concerns of this paper, the "hard core" of privacy protection rules in domestic legislation, enjoyed a substantial measure of consensus. Although the O.E.C.D. Guidelines reflect the influence of the language and presentation of the United States Privacy Study Protection Commission rather than the Council of Europe resolutions, the common themes are obvious. The points of difference from the Council of Europe draft Convention are less important than the points of similarity.

The O.E.C.D. Guidelines, as proposed to the Council, are in the form of an annexure to recommendations to be adopted by the Council addressed to member countries. These urge member countries to take the principles contained in the Guidelines into account in domestic legislation, to remove or avoid the creation of unjustified obstacles to trans border flows of

personal data, to co-operate in implementing the guidelines and to agree as soon as possible on a specific mechanism of consultation and co-operation.

The proposed Guidelines contain, after certain definitions and provisions as to their scope, exceptions from their operation and special rules applicable to federal countries with limited constitutional powers, Part Two which deals with the "basic principles" of national application. Part Three deals with certain basic principles of international application : free flow and legitimate restrictions. Part Four deals with national implementation. Part Five contains provisions concerning international co-operation. It is Part Two which is the subject matter of this examination.

Part Two contains eight paragraphs titled respectively (7) Collection Limitation Principle; (8) Data Quality Principle; (9) Purpose Specification Principle; (10) Use Limitation Principle; (11) Security Safeguards Principle; (12) Openness Principle; (13) Individual Participation Principle and (14) Accountability Principle. Even in the language of the titles chosen, the intellectual debt of the Expert Group to the United States Commission can be clearly seen. The origin of this influence may be explained by the fact that, when an impasse was reached in the deliberations of the Expert Group between the European members (who favoured language very similar to the Convention language of the Council of Europe) and the United States, the United States representatives were set the task of preparing what they saw as the basis of acceptable Guidelines for adoption in an O.E.C.D. context. Inevitably, the United States representatives looked to the most recent endeavour in their own country to provide a "conceptual framework" for legislation on the protection of privacy in information systems. This was the report "Personal Privacy in an Information Society". Having proposed for adoption the eight principles identified by that Commission, the onus then shifted to the Europeans to propose modifications and variations to bring the United States principles into line with their own notions of the "hard core". A number of important modifications of the United States principles were agreed to.

But in the result, it emerged that, at least in this Part of the Guidelines, the differences between the United States concepts, as stated in the report, and the European concepts, as already contained in the Council of Europe draft, were not as significant as had been thought. More significant differences existed in relation to other Parts of the Guidelines, notably the basic principles of international application. These differences were not confined to a debate between the United States and European countries; but that issue is not under consideration here.

A superficial examination of this subject might raise questions as to the legitimate interests of the O.E.C.D. to identify the "basic principles". Such "principles" might typically be catalogued as relating to "human rights", not normally the subject matter of the concerns of the Organisation. Without debating the limits of the activities of the O.E.C.D. under its Convention, two specific concerns lay behind the establishment of the Expert Group and were kept in mind by it during its work. Each was of particular relevance to the purposes of the O.E.C.D. The first was the rapid development of privacy protection legislation which could accidently and unintentionally impede free flows of data between member countries. The second was the fear of "data protectionism" already mentioned.

What was proposed by the O.E.C.D. Expert Group was not a convention. Some purists, and some European representatives, concerned to find a legally enforceable solution to the competing obligations of inconsistent data protection laws, urged that until a convention was entered into, Guidelines would be of little value. However, four advantages of the O.E.C.D. Guidelines can be mentioned :

(a) First, the O.E.C.D membership is itself more geographically scattered and includes countries which have a great significance for automated processing and trans border flows of data, especially the United States and Japan.

(b) Secondly, the mandate of the O.E.C.D. Group was not limited to consideration of automated data, as has been the case in other international projects, including those of the Council of Europe and the European Communities. In terms it extended to non automated data.

(c) Thirdly, the mandate of the O.E.C.D. Group was not limited to flows of personal data but included in item (ii) a consideration of the implications of non-personal data flows.

(d) Fourthly, as to the form of the international instrument proposed, some countries took the view that a persuasive but non-binding recommendation was most appropriate for those countries which have not yet adopted or are still considering domestic data protection laws. In such countries, a convention might be premature but Guidelines might positively influence the direction of domestic law-making. In itself, this could be a contribution to the harmonisation of laws in an area where the universality and pervasiveness of the technology involved suggest the need for harmonisation or at least the compatibility of laws. The possible need at a later stage to develop binding international conventions on data protection in the context of trans border data flows was generally acknowledged but considered distinctly premature by some.

Other International Organisations. The three international organisations now mentioned do not exhaust the efforts at an international level to develop principles on data protection and security. It is beyond the scope of this contribution to detail the work of the Nordic Council or the various non-governmental organisations such as the International Federation for Information Processing (I.F.I.P.) and the Intergovernmental Council of Automated Data Processing (I.C.A.).[40] Within the United Nations, the General Assembly adopted in December 1968 a resolution inviting the Secretary-General to undertake a study of human rights problems in connection with the developments of science and technology

generally. A preliminary report was submitted in 1970 to the Commission on Human Rights. Although the issue has been before the General Assembly on a number of occasions during the 1970s (and there has been certain relevant work within U.N.E.S.C.O.), the work within the United Nations has basically been addressed at the problems of developing countries. There is less concern in developing and socialist States about the perceived perils of invasion of privacy.[41] Their major concerns have been to secure the benefits of computerisation and technological development. Nevertheless, the relevant provisions of the International Covenant on Civil and Political Rights have already been mentioned. The international, universal nature of telecommunications-linked data banks will probably impose an obligation to develop international law applicable beyond the membership of the Council of Europe, the European Communities and the O.E.C.D.

I now turn to an identification of ten recurring suggested principles of privacy protection. These do not coincide precisely with the catalogue proposed within the O.E.C.D., the Council of Europe or the European Communities. Nevertheless, as will be seen, they closely approximate both the general principles put forward by these organisations as the "hard core" for adoption in privacy legislation and specific measures enacted in legislation of those countries which have already passed data privacy laws.

The ten suggested "basic principles" of information privacy are, in brief :

(1) The Social Justification Principle
(2) The Collection Limitation Principle
(3) The Information Quality Principle
(4) The Purpose Specification Principle
(5) The Disclosure Limitation Principle
(6) The Security Safeguards Principle
(7) The Policy of Openness Principle
(8) The Time Limitation Principle
(9) The Accountability Principle
(10) The Individual Participation Principle.

TEN PRINCIPLES OF DATA PRIVACY PROTECTION

The Social Justification Principle. The first principle proposed is a controversial one, not found in all international statements and not included in all national laws.

> The collection of personal data should be for a general purpose and specific uses which are socially acceptable.

The O.E.C.D. Guidelines do not contain reference to this principle. The preamble to the Council of Europe draft Convention refers to the common respect of member countries in "the Rule of Law as well as human rights and fundamental freedoms". Article 5(b) requires that personal data to be automatically processed shall be stored for specified "and legitimate" purposes and not used in any way incompatible with those purposes. In Australia, the N.S.W. Privacy Committee's Guidelines for the Operation of Personal Data Systems proposed a first division in relation to the operation of a personal data system, namely "the justification for the system". The first and second proposed rules refer to the social acceptability of the system's purposes and uses and the relevance and social acceptability of the data for specific decisions. The N.S.W. Committee proposed that as a general principle :

> a personal data system should exist only if it has a general purpose and specific uses which are socially acceptable.[42]

By "general purpose" the Committee explained that it meant the most abstract system of objectives. By "specific uses" was meant the operational objectives. It was pointed out that "social acceptability" was not synonymous with "legality". Some "unacceptable" forms of behaviour, including information collection and use, may be perfectly lawful but not socially condoned. The Committee admitted that the question of what constituted "social acceptability" was not a simple matter. No attempt was made to define what purposes and uses were or were not acceptable. The point being made was this. Privacy protection is not simply a matter of information efficiency. It has at its heart a matter of morality, concerned with individual liberties (as the French legislation, in terms, describes it) and "fairness" to the individual data subject.

It is for that reason that proposals have been made for the operation of a test of legitimacy and acceptability for the system and the uses of data within the system. In a sense, this threshold question asks in a general way what is later addressed by more specific principles in particular chronological stages. It is a question which is asked and answered in a number of the domestic laws of European countries. Certain particular kinds of personal information are identified as especially "sensitive". In such cases, strict limitations and even prohibitions are placed upon the "processing" of that particular kind of personal information.

The debate about whether particular classes of information should be identified as specially deserving of data protection exercised the O.E.C.D. Expert Group. In the end, despite arguments to the contrary by certain European countries, the consensus was that it would be impossible to reach an agreement among the differing cultural values represented, concerning those kinds of data that could be universally described as "specially sensitive". Furthermore, some participants took the view that it was the use and context rather than the nature of data that gave rise to perils against which privacy legislation should guard the individual. The Council of Europe draft Convention does identify a class of "sensitive data". Article 6 provides that personal data revealing religious or political opinions or racial origins or relating to criminal convictions may not be stored or disseminated unless domestic law provides appropriate safeguards. The European Parliament resolution, without defining the content, urges that the acquisition of "especially sensitive data" shall be subject to consent of the person concerned or to special legal authorisation.[43]

In a number of national laws particular data collections are singled out and identified as specially sensitive and therefore socially unacceptable, at least without specific safeguards and protections for the individuals concerned. Section 1 of the French law provides that data processing is to be at the service of every citizen, is to develop in the context of international co-operation and is to infringe neither human identity nor the rights of man nor privacy nor

individual or public liberties. Against this background, the French law proceeds to deal specifically and in terms with certain personal details considered particularly sensitive. Typical is the provision of s.31 which provides that without a party's express consent, the recording or storage in a computer memory of personal data which directly or indirectly reflects racial origins or political, philosophical and religious opinions or Union membership is prohibited.[44]

The provisions in the French law are reflected in the laws of other European countries. The Swedish Data Act commences with a provision in s.2 that a collection of personal information may not be started or kept without permission of the Data Inspection Board. By s.3 the Board may grant its permission if there is no reason to suspect that undue encroachments on the privacy of individuals may arise. Section 4, however, makes special provisions in respect of "sensitive" personal data. These include lists of criminal convictions or sentences, details of coercive action under the Child Welfare Act, the Temperance Act or mental health laws, details of personal illness, the receipt of social assistance, treatment of alcoholism and so on. Permission to start and keep a register containing personal information about the person's political or religious views may be granted only where there are "special reasons". Similar provisions are found in the Danish and Norwegian legislation.[45]

Not surprisingly, the Council of Europe Draft Convention reflects this specific concern in Article 6. Although the O.E.C.D. Guidelines do not adopt the attempt to define specially sensitive data they do, in dealing with the scope of their operation, make reference to the competing views as to what it is that makes personal data specially dangerous. According to paragraph 2, the Guidelines apply to personal data which, because of the manner in which they are processed [the automated v. manual issue] or because of their nature [especially sensitive facts issue] or the context in which they are used [the official United States view] pose a danger to privacy and individual liberties.

The Australian Law Reform Commission, in its report on Unfair Publication reflected, in that special context, the majority European view. An attempt was there made to identify, for the purposes of controlling publication, certain aspects of personal life which were considered to be in need of special protection. The aspects identified are much narrower than the concerned listed in the Council of Europe draft Convention or the European legislation just quoted. There is no mention for example of religious or political opinions or racial origins. Instead, the information defined as "specially sensitive" relates principally to a person's family, home and sexual life and personal associations. The common feature is the assertion that some information about a person, even if of general interest or relevance, ought not to be collected, used or disseminated because it is not socially acceptable to do so. At the heart of this assertion is a conviction of the danger to individual freedoms in the use of such information, even when consideration is given to the value of the information. The N.S.W. Guidelines put the point thus :

> In some circumstances, even though the information is relevant, its use in certain decision-making situations may be prohibited by law or be so socially unacceptable. This is the intent of racial and sex anti-discrimination provisions and some criminal rehabilitation proposals. Community standards also largely preclude questions on religious and political affiliations. The reason for such prohibition is the sensitivity of the data, by which is meant the importance which a given person places upon the non-disclosure of a given item of information.[46]

This is a controversial issue and one upon which the O.E.C.D. Group with its wider membership reflecting different cultural values could not reach unanimous agreement. Symbolic of this is the fact that although the proposed Australian legislation on publication privacy identified certain information as specially sensitive, the field so identified is different from that identified as prima facie sensitive and illegitimate in the Council of Europe Committee. The Australian specification reflects an Anglophone concern about family, friends, bodily health and sexual morality. The European list, with memories of the War still fresh, reflects other phenomena which, even in quite recent European history, were literally matters of life and death for the data subject.

The Collection Limitation Principle. Less controversial is the proposal that, as a "basic rule" of privacy protection there should be limits on the collection of personal data :

> The collection of personal data should be restricted to the minimum necessary and such data should not be obtained by unlawful or unfair means but should be collected either with the knowlege or consent of the data subject or with the authority of law.

Both the O.E.C.D. and Council of Europe texts address this principle. Paragraph 7 of the O.E.C.D. Guidelines provides that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject. The Council of Europe text is limited to automatically processed data. But the principle is much the same. Article 5(a) requires that personal data to be automatically processed shall be (a) obtained and processed fairly and lawfully and (c) adequate relevant and not excessive in relation to the purposes for which they are maintained.

In the Australian Law Reform Commission's report on Privacy and the Census[47] the Commission endorses the adoption of the general principle that an individual should not be required to provide personal information which is not relevant to and necessary for the purposes of the collection. The Guidelines of the N.S.W. Privacy Committee suggest that in general the minimum data necessary to achieve the purpose is all that should be collected. Speculative collections of personal data (on the grounds that they just might be needed later and would be more economically collected now) should be avoided.[48]

Apart from dealing with the quantity of information, the second principle also deals with the person from whom personal data should be collected. A reflection of the suggested principle that the consent of the data subject should normally be obtained is found in most drafts. The European Parliament resolution draws a distinction between personal data and specially sensitive data. The former should be obtained by lawful means. The latter should be acquired only with the subject's consent or special legal authorisation.[49]

The principles of "collection limitation" are reflected in numerous provisions of domestic data protection law. In the United States Privacy Act, for example, Federal agency maintenance of a system of records is limited to those records only with such information about an individual "as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President".[50] It is also provided that such agencies should collect information to the greatest extent practicable directly from the subject. This last requirement is limited to cases where "the information may result in adverse determinations about an individual's rights, benefits and privileges under federal programs".[51] Such provisions are in line with the statement of purposes contained in the Act. To protect the individual, except as provided by law, he is himself to determine what records pertaining to him are collected, maintained, used or disseminated by federal agencies.[52]

A similar approach is taken in the Canadian federal statute. There is a specific declaration against unnecessary collection of information for storage and an obligation to review proposals for the creation of new personal information banks.[53] Section 2 of the Canadian Act permits the making of regulations prescribing any special procedures to be followed by a government institution in obtaining personal information for inclusion in a federal information bank.

A number of the European laws forbid and punish the dishonest, fraudulent or illegal acquisition of data.[54] Most make specific provision in relation to collections of particular kinds of "sensitive" data. Several make it plain that special authorisation of law may be appropriate as an alternative to individual consent in some cases for the collection of personal data.[55]

The Information Quality Principle. The third "basic rule" is also a comon recurring theme.

> Personal data should, for the purposes for which they are to be used, be accurate, complete and kept up to date.

The O.E.C.D. definition of this principle is almost identical. Paragraph 8 of the O.E.C.D. Guidelines requires that personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up to date. The Council of Europe draft Convention, although limited to automatically processed personal data, is very similar. It requires that such data should be adequate, relevant and not excessive in relation to the purposes of the data file and "accurate and, where necessary, kept up to date".[56] It is to be noted that there is no obligation of automatic updating in any of these texts. The proposed principle and the O.E.C.D. Guidelines take as their touchstone the necessity arising from the purposes for which personal data are to be used. The Council of Europe text, without defining that necessity, limits the obligation to maintain up-to-dateness to "where necessary".

The resolution of the European Parliament is in more peremptory terms :

> Personal data to be processed
> - may be recorded and transmitted only for the designated purposes and in confirmity with the declaration made by, or the authorisation granted to, the data controller : the data protection body must be empowered to permit exceptions;
> - shall be accurate and necessary for the purpose for which the data bank has been established.[57]

In the Australian proposals so far developed, reference is made to the requirements of data quality of accuracy, timeliness and completeness.[58] Furthermore, specific provisions in a number of national laws illustrate the way in which the requirements of information quality are addressed. In the United States Privacy Act one of the purposes of the Act, is declared to be the provision of safeguards for individuals against invasion of personal privacy by requiring federal agencies to ensure that information is "current and accurate for its intended use".

Specific provisions are then included in the Act in terms which are mandatory and addressed to federal agencies. For example agencies are required to maintain all records which are used by the agency in making any determination about an individual "with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual in the determination".[59] Section 36 of the French law asserts that the data subject may require the correction, alteration, clarification, updating or erasure of data concerning him which is :

> inaccurate, incomplete, ambiguous, outdated or of which the acquisition, use, disclosure or storage is prohibited.[60]

Similar provisions are to be found in other national laws. For example, s.8 of the Swedish Data Act provides that if there is reason to suspect that personal information in a personal register is incorrect, the responsible keeper is obliged without delay to take the necessary steps to ascertain the correct facts and, if necessary, to correct the record or exclude information from it. Section 4 of the German Act[61] provides that subject to the Act every person is entitled to the erasure from storage of data concerning him where the original storage was inadmissable or where the original requirements of storage no longer apply.[62]

The Purpose Specification Principle. The fourth principle relates to the individual's control over the use made of personal data about himself :

> The purposes for which personal data are collected should be specified to the data subject not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

This principle has been taken from paragraph 9 of the O.E.C.D. Guidelines. In the Council of Europe draft Convention the same idea is expressed in the requirement that personal data to be automatically processed shall be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes".[63] Although the two statements are similar, there is a signficant difference. The Council of Europe statement forbids in broad language subsequent use of the data

in a way that is incompatible with the original specified use on the basis of which it was collected. The O.E.C.D. Guidelines are more specific. They would require limitation to the fulfilment of the original specified purpose or such others as are [openly] specified from time to time by the information keeper. No mention is made of the legitimacy of the purposes, an omission which has already been commented upon. The European Parliament resolution limits transmission to designated and declared purposes or if authorised by the data protection body. Specifically, the resolution provides that the amalgamation in whatever form of separate data banks "shall require the consent of the data protection body".[64]

In the Australian Law Reform Commission's report on privacy protection in the census, the "purpose specification principle" was adopted in terms. An individual should be informed of the purposes for which personal information is being collected from him. He should be told of the uses to which the information may be put and the consequences, if any, attached to a refusal to supply it.[65] Detailed recommendations are made concerning improvement of purpose specification including the groups needing special care such as ethnic minorities and Aboriginals. The N.S.W. Guidelines also contain provisions relevant to the specification of purposes and limitation of uses to such purposes.[66]

The principle of requiring the collector of personal information to specify uses and later to adhere to that specification (unless varied by consent or authority of law) is also reflected in a number of domestic legislative provisions. For example s.9(2) of the Federal German law requires that where data are collected from a person on the basis of a legal provision. The subject's attention shall be drawn to such provision and in all other cases he shall be informed that he is not obliged to provide the data. Section 27 of the French law requires not only specification of any compulsory character of the collection but also identification of the persons for whom the data are intended and the rights of access conferred.[67] The United States Privacy Act includes amongst its declared purposes the requirement that unless exempted by law, federal agencies should permit an individual to "prevent

records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent."[68] The provisions of this stated purpose of the legislation are spelt out in some detail in the Act which imposes on the agency the obligation to inform the individual of the authority, purpose and use to which the requested information will be put.[69]

The Disclosure Limitation Principle. The fifth principle is designed to limit the circulation of personal data to a specified and proper class of case :

> Personal data should not be disclosed or made available except with the consent of the data subject, the authority of law or pursuant to a publicly known usage or common and routine practice.

The O.E.C.D. Guidelines in paragraph 10 describe this as the "Use Limitation Principle". According to this principle, personal data should not be disclosed, made available or otherwise used for purposes other than those specified [initially or on change of purpose] except with the consent of the data subject or by the authority of law. The Council of Europe text is less dogmatic on this point, requiring mere compatability of use. Article 5(b) requires that personal data to be automatically processed shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. The provisions of the relevant part of the European Parliament resolution have been cited above.

In Australia, the Law Reform Commission has attempted, in a research document, to specify the kinds of cases where disclosure of personal data supplied for a different purpose may be legitimate even without the prior consent of the data subject. The case of disclosure to a legal representative was one case mentioned but may be dismissed as being within the rubric of consent. But other disclosures are contemplated, namely disclosure in response to a formal legal process, for audit purposes, in an anonymous form for statistical or research purposes and "where there are compelling reasons relating to the health or safety of the subject".[70]

The N.S.W. Privacy Committee's Guidelines assert as the general rule that personal data should only be accessed consistently with the system's uses and "for additional uses by consent or by law".[71] Among the principles for fair access to personal data are listed consent which is informed and not given under any physical or psychological duress, access which is legally authorised (as for example by the Taxation Office under federal tax legislation[72]) and what are described as "emergency uses". The Privacy Committee was prepared to allow an exceptional entitlement of access, even without consent or specific authority of law, where to fail to allow access would be "likely to be a significant factor in serious physical or emotional harm occurring to some persons".

Numerous provisions in domestic legislation deal specifically with the disclosure of personal data for fresh purposes. The Austrian law provides a list of exceptions to the case of non-disclosure of data provided by private legal entities. The exceptions include express written consent, fulfilment of the legitimate objects of the person responsible, necessity of a third party (for the protection of the over-riding and legitimate interests) and de-identification.[73] An additional provision in s.18(2) exempts cases where there is a legal duty to disclose data. Sub-section 18(5) exempts disclosure to the Central Statistics Office solely for statistical purposes for processing in anonymous form. In the French law, a criminal offence occurs where a person knowingly and without authorisation of the subject discloses personal data.[74] Section 52 of the Canadian Act and s.552(a)(b) of the United States Privacy Act spell out even more specifically the disclosure limitation principle. In the United States Act, consent of the data subject is required unless the disclosure of the record would be to officers of the agency performing their duties, for a "routine use" as defined, to the Bureau of Census for statistical research, to the National Archives or to another government agency for civil or criminal law enforcement and then only if the head of the agency has made a written request.[75]

It seems commonly acknowledged here that there should be limitations upon the use made of personal data supplied for a specific purpose. The limitation upon putting such data to a different use arises from the fact that data might have been supplied in a different form, fuller and in greater detail had it been known that it would be used for a different purpose. The building of composite profiles from linked data is also addressed by this principle as is the desirability of individuals keeping general control over how they are perceived and by whom. But whilst the principle is acknowledged, exceptions must also be allowed for. It is easy to contemplate exclusion in the case of knowing consent and specific authority of law. Beyond that, the exceptions are more problematical. To avoid needless, inefficient recourse to the data subject for his consent, some provision seems appropriate for uncontroversial, innocuous and routine use. The Council of Europe draft seeks to accomplish this by use of the notion of "compatability". An alternative is to incorporate, as in the United States legislation, an elaborated notion of "routine" or "common" practice. The use of a telephone book entry, for example, for purposes other than identification of the telephone number of the subject, should not require constant access to the data subject for his consent. Much more controversial is the exception for emergency cases and particularly emergencies involving third parties. As acknowledged by the N.S.W. Privacy Committee itself, a too generous use of this exception could entirely undo the protection contemplated by the fifth principle.

The Security Safeguards Principle. The obligation to provide adequate data security is a common theme of every international statement and all domestic legislation. Only the nuances are different :

> Personal data should be protected by security safeguards which are reasonable and appropriate for the purpose of preventing loss, destruction, unauthorised access to, use, modification or disclosure of data.

The differences between the proposed formula and paragraph 11 of the O.E.C.D. Guidelines are unimportant. In the latter, the requirement is to provide "reasonable security safeguards" but no referent is provided as above. Furthermore, the wrongful acts are listed as examples of the risks against which

reasonable security safeguards should be implemented. The Council of Europe statement of the principle is in almost identical language. Article 7 relating to data security provides that appropriate measures shall be taken for the protection of personal data recorded in automated data files, against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

In the Australian Law Reform Commission on Privacy and the Census the Commission endorsed a principle that the methods used to collect information "should be such as to minimise the danger of unauthorised or unwarranted disclosure of that information".[76] Various specific recommendations were made to translate these general comments into detailed obligation. The need to protect the security of personal information supplied for the Census, while still in identifiable form, was addressed in some detail. The N.S.W. Privacy Committee's Guidelines propose that there should be included the establishment and maintenance of standards regarding data security.[77] Levels of security should be commensurate with the sensitivity of the data. No security measures can be regarded as foolproof.

In national legislation, a number of laws give attention to the security of personal data. For example, the Austrian law provides that any person has the right to demand that personal data concerning himself be kept secret provided that he has an intesting warranting protection, notably "as concerns respect for his private and family life".[78] Section 29 of the French law is stated in terms of obligations and is reinforced by the provision of criminal sanctions. A person processing personal data is taken to have given an undertaking to the persons concerned that he will see that "all necessary precautions are taken to protect the data and in particular to prevent them from being distorted, damaged or disclosed to unauthorised third parties".[79] Failure to do so renders the record keeper liable to penalty. The United States Privacy Act also contains an obligation on federal agencies to establish rules of conduct for persons involved in information systems.[80] By administrative, technical and physical safeguards, the security and confidentiality of records is to be ensured.[80]

The most ambitious national law on this subject is the German Federal Act. There, an attempt is made to list, in respect of data processed automatically, appropriate measures which are to be taken to ensure the observance of the provisions of the Act. Ten principles are collected which lay down rules for the control of admission to facilities, removal without authorisation, unauthorised modification, unauthorised use, unauthorised access, unauthorised dissemination, unauthorised input, unauthorised processing for other parties, unauthorised access during transport and the implementation of appropriate control within the organisation.[81]

The Policy of Openness Principle. The seventh principle is also a common theme :

> There should be a general policy of openness about developments, practices and policies with respect to personal data. In particular, means should be readily available to establish the existence, purposes, policies and practices associated with personal data as well as for the purpose of establishing the identity and residence of the data controller.

Paragraph 12 of the O.E.C.D. Guidelines is in terms almost identical to the above suggested principle, which is in turn drawn from the first two rules of the H.E.W. code of fair information practices. The Council of Europe draft Convention, in Article 8, lists certain "additional safeguards for the data subject". They include the right of "any person" to be enabled :

> (a) to establish the existence and main purposes of an automated personal data file, as well as the identity and habitual residence of the controller of the file.

The general philosophical principle of openness is omitted but the specific and important machinery provisions are in terms parallel to the proposed principle and the O.E.C.D. Guidelines.

The European Parliament resolution is at once more narrow and more imperative. In terms, the obligation in Part II (where the relevant provision is found) is limited to "persons whose usual residence is in the territory of a member State". Only such persons should have the listed rights. The Council of Europe Draft affords the right to "any person". In the O.E.C.D. Guidelines, the right enures in an "individual".

Paragraph 8(a) of the European Parliament resolution proposes that such persons should have the right "to information on all measures involving the recording, storage or transmission to third parties of data relating to them and on the contents, purpose and recipient thereof". Paragraph 4 of the resolution would require data controllers to inform the person concerned when personal data are first stored. The general policy of openness and the provision of facilities readily to ascertain the whereabouts of a data controller are not addressed, except by imposing obligations on the data controller. The problem of the non-observance of these obligations by him is not dealt with.

In Australia, the N.S.W. Privacy Guidelines include the general principle that "the interested public" should be able to know of the existence, purpose, uses and methods of operation of pesonal data systems.[82] In national legislation requirements for compliance with the "openness principle" are common. For example, the United States Privacy Act provides an obligation on federal agencies, with certain exceptions, to publish at least annually in the Federal Register a notice of the existence and character of the systems of records. Various details, designed to facilitate inquiries and access, are also to be published.[83] In a similar vein are the provisions of the Canadian legislation which have led to the production of the Index to Federal Data Banks in Canada.[84] The openness principle is also reflected in the legislation of Western Europe. Under the German Federal Act, the Federal Commissioner is required to keep a register of automatically operated data files in which personal data are stored. This register is to be open to inspection by any person. Public authorities and other bodies subject to the Act are required to report to the Federal Commissioner details of the data files which are automatically processed by them. Certain security and intelligence organisations are exempt.[85] Under s.22 of the French Act, the National Commission established by the Act is obliged to make a list of the processing activities accessable by the public, specifying in each case the law authorising the collection, how access is to be provided, categories of personal data recorded and rulings, opinions or recommendations of the Commission that may be relevant. Under s.34 of the

French Act, any person proving his identity is entitled to obtain from departments and organisations using automatic processing a list of similar information. The Austrian Act imposes upon the Austrian Central Statistics Office an obligation to keep a data processing register.[86] This register is to be open for inspection by any person and is to contain the list of all personal information systems authorised under Austrian law.

The Time Limitation Principe. The eighth principle is more controversial. According to it :

> Personal data in a form which permits identification of the data subject should, where the purposes of the data have expired, be destroyed, archived or de-identified.

The O.E.C.D. Guidelines make no reference to the limitation of the time during which identifiable personal data may be retained. In an earlier draft of the Guidelines provision was made for erasure or conversion into an anonymous form (unless needed for research or archive purposes) of personal data which no longer serves current purposes. The O.E.C.D. Expert Group decided to delete this provision. The ground included that the information quality principle and the principles limiting the use of personal data effectively did the work of time limitation, without imposing an expensive and possibly even privacy-harmful obligation of culling and destroying personal information. On the other hand, other international and national approaches have recognised the specific dangers of indefinite, perpetual collections of personal data. By becoming out-dated such data may become inaccurate or unfair, causing disproportionate potential harm to the data subject. This approach would appear to be reflected in Article 5(e) of the Council of Europe draft Convention. This requires that personal data to be automatically processed shall be "preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are maintained". The European Parliament resolution is even more emphatic. Paragraph 2 requires that personal data to be processed "shall be erased whenever they ... are inaccurate or out of date, or as soon as the purpose for which they were recorded has been achieved".[87]

In Australia, the most massive example of the adoption and application of a time limitation principle in respect of personal data files is the complete destruction of the original census returns and of the personal identifiers which link returns to de-identified statistical data. Unlike most countries, where Census information is retained under strict archival security, the Australian practice has been to de-identify the data within a short time of collection and then to destroy the identifiable returns, their purpose (the supply of statistics) having been completed. In its report, the Law Reform Commission suggested that, for a number of reasons, this application of the time limitation principle was excessive. It was proposed that for future medical research, historical inquiry and genealogical investigations, the identified data should, as in other countries, be retained under strict conditions of archival confidentiality, with limitations upon access for 75 years. This proposal was not accepted by the Australian Government. In the Federal Treasurer's statement to Parliament, there is evidence of the strongly felt view of the propriety of destroying certain personal data, when its purposes have been fulfilled :

> The Government has carefully weighed the arguments for and against the proposal [of non destruction] and has decided not to accept it. The purpose of the Census is to gather statistical information and the legal obligation on people to answer Census questions ... is accompanied by strict measures to ensure the confidentiality of the information provided. The Government believes that it would be inconsistent with that purpose and with the guarantee of confidentiality to retain information on identified persons or households for the research purposes referred to in the Commission's report. Consequently the present practice of destroying all records of names and addresses and of not entering into the computer records such names and addresses will be continued.[88]

In the N.S.W. Guidelines, the Privacy Committee proposed that identified personal data should only be retained as long as a use remains, after which it should be either destroyed or de-identified or archived.[89]

In national legislation, the principle of limiting the duration of the retention of identifiable personal records is frequently provided for. The U.S. Privacy Act provides

specifically for archiving records.[90] Transfer to the National Archives is considered, for most purposes, an adequate protection for individual privacy. The time limitation principle is expressed in s.8 of the French legislation :

> 28. Unless otherwise provided by law, data may not be stored in a personal form beyond the period stated in the application for opinion or in the declaration, unless such storage is authorised by the Commission.

Under the Swedish Data Act the Data Inspection Board may limit permission to start a register of personal information to a certain period of time. Under the Danish Public Authorities Act, where personal data becomes obsolete, the Minister may, after consultation with the Data Surveillance Authority, deposit the information for safe custody in the Archives subject to such conditions as are laid down.[91]

The Accountability Principle. There is less debate about the need to identify someone as responsible for complying with privacy laws. The proposed ninth principle is :

> There should be, in respect of personal data, an identifiable data controller who should be accountable in law for giving effect to these principles.

Both the O.E.C.D. Guidelines and the Council of Europe Draft Convention have addressed themselves to the practical need to assign administrative, and ultimately legal, responsibility for ensuring compliance with requirements of data protection. The problem arises specfically in the case of corporations which act through their servants and agents. It also arises as an acute problem in the case of service bureaux, where the nature of the functions of the bureaux may exclude appropriate legal and moral obligations to ensure compliance, with the principles of privacy protection of the data being processed. The O.E.C.D. Guidelines are in terms similar to the above statement of the principle. The Council of Europe text confines itself to enabling a person to identify and find the habitual residence of the controller of the file. This "controller" is defined to mean the natural or legal person, public authority, agency or any other body "which is competent to decide what should be the purpose of the automated data file, which categories of personal data should be recorded and which processes should be applied to them". The resolution of the European Parliament is

more emphatic but less specific. Paragraph 3 provides that the data controller (undefined) shall be liable for material and non-material damage caused by the misuse of data, whether or not there was any negligence on his part.[92]

In Australia, proposals for the identification of an "information manager" to be appointed by record-keepers and with whom a subject can deal in relation to his data rights, have been explored by the Law Reform Commission. The N.S.W. Guidelines do not deal specifically with this subject, perceiving it as an aspect of the "openness principle" or the "individual participation principle". In the N.S.W. Guidelines, the "system operator" is defined as the "person or organisation by whom or on whose behalf a personal data system is operated".

In national legislation, it was recognised from the first that practical privacy protection would require the identification of an accountable data controller. The Swedish Data Act in its first section provides for accountability. It defines as a "responsible keeper of a file" anyone "for whose purposes a personal file is kept, if the file is at his disposal".[93] The responsible keeper is required to register with the Data Inspection Board. It is upon him that the obligation rests to keep the Board notified of specified matters relevant to the protection of privacy. It is he who is obliged to deliver information and particulars to the Board as required. However, certain provisions of the Act are also expressed to apply to anyone who handles a personal register on behalf of the responsible keeper.[94] The most specific legislation dealing in detail with the appointment of a data controller is to be found in the Federal Republic of Germany.[95] Specific duties are cast upon the "controller of data protection".[96] Further, specific duties are imposed on all persons "engaged in data processing". All such persons are required, for example, to give an undertaking to abide by the general duties imposed by the Act.[97] A similar requirement that persons to whom data are entrusted in the course of their employment should expressly undertake to respect the confidentiality of such data is provided in the Austrian Act.[98] As in the German legislation, criminal sanctions are

provided for breach of the undertaking, enduring after the termination of employment. The Austrian Act, however, proceeds to attempt to protect an employee against unlawful orders of an employer.

> (20)(4) The refusal of an employee to carry out an order which would involve a violation of the confidentiality of data shall not result in any prejudice being suffered by such employee.

It has often been said that the criminal law is necessary as a protection for the "front line" data operator who becomes aware of the performance of unlawful or unfair invasions of privacy in the course of using a personal data system. The Austrian provision provides an alternative or supplementary measure to the low level data operator. However, its method of enforcement is far from clear.

The Individual Participation Principle. Finally, the tenth principle is perhaps the most important. It has already been described as the "golden rule" of data protection. It is happily common to international statements and national legislation and in Australia it has already been endorsed as a general rule by the inquiry of the Law Reform Commission. The tenth principle may be stated as follows :

> An individual should have a right :
> (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
> (b) to have communicated to him, data relating to him :
> (i) within a reasonable time
> (ii) at a charge, if any, that is not excessive
> (iii) in a reasonable manner; and
> (iv) in a form that is readily intelligible to him
> (c) to challenge data relating to him and :
> (i) during such challenge to have the record annotated concerning the challenge; and
> (ii) if the challenge is successful, to have the data corrected, completed, amended, annotated or, if appropriate, erased; and
> (d) to be notified of the reasons if a request made under pararaphs (a) and (b) is denied and to be able to challenge such denial.

So far as international statements of the core principles are concerned, the language proposed above follows substantially pararaph 13 of the O.E.C.D. Guidelines. The only variants are a specific provision for annotation of the record during challenge (perhaps a matter of machinery). The Council of Europe formulation lists the right of individual participation in Article 8, which collects the "additional safeguards for the data subject". The differences are matters of emphasis. In addition to the ability to establish the existence of the file and the identity and habitual residence of the controller, already referred to, three additional entitlements are listed. These are the power to obtain "at reasonable intervals and without excessive delay or expense" confirmation of whether personal data are stored as well as communication of such data in intelligible form; where appropriate, rectification or erasure of data processed contrary to the basic principles and to have a remedy if these entitlements are not complied with.

The European parliament resolution would provide that all persons whose usual residence is in the territory of a member State should have the right to have personal data erased where conditions of data quality are not fulfilled, unless the data controller can prove the opposite; to have inaccurate or incorrect data corrected and third parties to whom such data have been transmitted informed accordingly; and to require the data control body to check the legality of data relating to them.[100]

In Australia, the principle of subject access was endorsed in the Australian Law Reform Commission's report on the privacy aspects of the Census.[101] A number of reasons were advanced :

> The Commission endorses the basic principle that an individual should normally be allowed to have access to and to challenge, a record of personal information about him. This principle is based on two main considerations. First, a personal record affects the way in which an individual is perceived by others. It creates the image which the individual has for the record-keeper and for other persons who use the record. Secondly, access provides a unique means for monitoring the record-keeper's compliance with the standards applicable to the collection and use of information. It provides an opportunity for

> correcting errors affecting the individual's interests. The principle of access is a central aspect of privacy legislation and proposals in both Europe and North America.[102]

The N.S.W. Guidelines also adopt the general right of subject access. The provisions governing personal access by the data subject, and machinery for upholding that access, is a common feature of data protection and privacy laws so far enacted. The United States Privacy Act includes, as one of its purposes, the provision of safeguards against invasions of privacy by federal agency files so that, except as provided by law, agencies will permit an individual "to gain access to information pertaining to him in federal agency records, and to have a copy made of all or any portion thereof and to correct or amend such records".[103] The machinery to provide access is spelt out in sub-title (d). On request of any individual, agencies are required to permit him to review the record and have a copy made, to permit the individual to request amendment to comply with such a request or inform the individual of refusal and to permit the individual who disagrees with the refusal to have an internal review and final determination made, subject to judicial review.[104] A similar provision is contained in the Canadian Act.[105]

The above provisions are also reflected in European legislation. Under the French law any person proving his identify is entitled to question department or organisations using automated processing and to receive a list from which he can determine whether such processing involves personal data concerning himself. If such data does concern himself, he is entitled "to obtain access thereto".[106]. The law then provides for the machinery of access including intelligibility of the data supplied, the fee charged[107] and right of completion, correction, clarification, updating or erasure. In the event of a dispute the onus of proof is generally to be on the department. Where the holder of a right of access causes the record to be altered, the charge he has paid is to be refunded.[108]

The Federal German Act makes similar provision, declaring the rights of the data subject in broad language at the outset of the Act :

s.4 Subject to the provisions of this Act every person shall be entitled to :

1. information on stored data concerning him;
2. correction of any incorrect stored data concerning him;
3. blocking of stored data concerning him where the accuracy or inaccuracy cannot be established or where the original requirements for their storage no longer apply;
4. erasure of stored data concerning him where such storage was inadmissible or - as an option to the right to the blocking of data - where the original requirements for storage no longer apply.[109]

There are like provisions in the Austrian, Swedish Danish and Norwegian laws. Indeed this is a common provision to be found in data protection laws of Europe, the United States and Canada. The machinery for enforcement differs. In the United States the machinery, other than internal bureucratic review, is principally a civil action for damages and, in a limited number of cases, criminal penalties. In Canada, the machinery provided is complaint to the Privacy Commissioner who has Ombudsman-like powers of persuasion and report to Parliament. In Europe, provision is typically made for complaint to a data protection authority, with powers of specific order to secure compliance, in some cases report to Parliament and generally criminal penalties of fine and imprisonment in the case of more serious and wilful breaches.

CONCLUSIONS

The limitations of this study are obvious. The principal international instruments on trans border data flows have not yet been concluded. The European Community is awaiting the outcome of the work of the Council of Europe. A draft Convention of the Council has not yet been finally passed upon. Within the O.E.C.D., although substantial consensus has been achieved in the Expert Group, a number of outstanding reservations remain to be resolved at a political level. Within Australia, the inadequacies of current privacy laws are only now being addressed by the national law commission and various State inquiries co-operating with it. In many other countries, including countries vitally important for trans border data flows, privacy legisation is, as in Australia, still being

discussed and developed. To these elements of uncertainty must be added the dynamics of the fast-changing technology and the priorities assigned to data protection at a time when other concerns of the new information technology (unemployment, national sovereignty, energy conservation and cultural independence) compete for the attention of lawmakers.

The prognosis with which this essay was begun was a gloomy one. It was that laws for data protection would be bureaucratic and would abort otherwise desirable advances for mankind inherent in new telecommunications technology. Such a prediction might, even if true, be borne as the price paid for the defence of important individual liberties, including privacy protection. However, the second prediction was more disquieting. It was that, for all the efforts of law makers, data protection laws would not actually succeed in safeguarding privacy. There are some who urge that lawmakers should not impede technological process, especially where the technology promotes the greater flow of information which is generally conceded to be to the advantage of mankind. Pessimists put it another way. They assert that the puny efforts of lawmakers are likely to be ineffective and overtaken by events, causing no more than scattered, intermittent interruptions to the onward thrust of technological advance.

Some comfort can be taken by lawmakers and those who advise them from this study. Despite the enormous differences of language, culture and legal tradition, it is a remarkable fact that in the last decade a series of laws has been enacted with basically similar provisions, gathering around a number of identifiable "general rules". Of course, the rules are expressed in the broadest possible language. They contemplate different applications and in their generality they disguise many important unresolved debates.[110] Furthermore, nothing has been said of the exceptions from their operation. Specific to the issue of trans border data flows, nothing has been said concerning the principles of international application and how in the context of instantaneous universal technology effective protection can possibly be ensured.

For all this, it is reassuring that there is such commonality in the adoption, with a fair degree of consensus, of the "basic rules". It suggests that there is sense in the basic endeavour. The identification of the general principles by international bodies such as the O.E.C.D and the Council of Europe will not only be helpful for those countries which have already existing privacy protection laws to be measured against the agreed standard. It will also be useful as a benchmark for those countries, including Australia, which are in the process of developing such laws.

The inefficiencies and impediments to the information technology predicted by the gloomy futurologist may not be removed by the mere compliance with the "basic rules" of domestic legislation in numerous countries. But at least a potential source of bureaucratic rigidity and international impediments will be avoided if the domestic privacy protection legislation of developed countries adhere to a single conceptual framework. It is this belief which has motivated much of the work done in the Council of Europe and the O.E.C.D. For once, the gloomy predictions may be proved wrong. For the maintenance of a proper balance between flows of information and the legitimate protection of individual privacy, let us hope so.

FOOTNOTES

* Chairman of the Australian Law Reform Commission, 1975 - Chairman of the Expert Group on Trans Border Data Barriers and the Protection of Privacy within the Organisation for Economic Co-operation and Development (O.E.C.D.). 1978 - The views expressed are the author's personal views.

1. ECONOMIST, 29 December 1979, 10.

2. Swedish Data Act (Datalagen) 11 May 1973, s.11. The text of this and other non-English language statutes referred to is from the translation in a compilation of privacy legislation of O.E.C.D. member countries prepared by the O.E.C.D. Secretariat. Cf. Danish Private Registers Etc. Act (Lov om private registre) No. 293 of 8 June 1978 s.7; and Danish Public Authorities Registers Act (Lov om ossentlige myndigheders registre) No. 294 of 8 June 1978 s.20(3).

3. French law relating to Information Technology, Files and Liberties (Loi relative a l'informatique, aux fichiers, et aux libertes) of 6 January 1978 (hereafter French Act) s.24.

4. Statement made to the 24th Session of the Committee for Scientific and Technological Policy of the O.E.C.D., 21 November 1979, 5. The statement is an annex to the Summary Record of that session.

5. Australian Constitution, s.107.

6. Latham C.J. in Victoria Park Racing & Recreation Grounds Co. Ltd. v. Taylor (1937) 58 Commonwealth L.R. 479, 496.

7. Privacy Committee Act (N.S.W.)

8. For a description of the operations of the Australian Law Reform Commission and the implementation of its reports, see THE LAW REFORM COMMISSION, ANNUAL REPORT 1979 (ALRC Report No. 13), Canberra, Aust.Gov.Pub.Service, 1979.

9. PRIVACY COMMITTEE (New South Wales), GUIDELINES FOR THE OPERATION OF PERSONAL DATA SYSTEMS, exposure draft (B.P.31) April 1977, Sydney. Hereafter referred to as N.S.W. Guidelines.

10. See for example Census & Statistics Act 1905 (Aust.) ss.7, 22, 24; Income Tax Assessment Act 1936 (Aust.), s.16.

11. Telephone Communications (Interception) Act 1960 (Aust.), repealed and substituted by Telecommunications (Interception) Act 1979 (Aust.).

12. Listening Devices Act, 1969 (N.S.W.); Listening Devices Act 1969 (Vic.); Invasion of Privacy Act of 1971 (Queensland); Listening Devices Act 1972 (S.A.); Listening Devices Act 1978 (West Aust.). See also Listening Devices Bill 1974 (Tas.).

13. Invasion of Privacy Act of 1971 (Qld.); Fair Credit Reports Act 1975 (S.A.); Credit Reporting Act 1978 (Vic.).

14. THE LAW REFORM COMMISSION, CRIMINAL INVESTIGATION (ALRC Report No. 2 - Interim) 1975, Aust.Govt.Publishing Service, Canberra.

15. AUSTRALIAN PARLIAMENT, SENATE STANDING COMMITTEE ON CONSTITUTIONAL AND LEGAL AFFAIRS, FREEDOM OF INFORMATION (Report on Freedom of Information Bill and aspects of the Archives Bill 1978), 1979, Aust.Govt.Publishing Service, Canberra. See especially 263 where the desirability of a Right to Privacy Act is discussed.

16. A.L.R.C. Report No. 11, 1979, Aust.Govt.Publishing Service, Canberra.

17. Draft Unfair Publication Act, Clause 3(1) in THE LAW REFORM COMMISSION, UNFAIR PUBLICATION : DEFAMATION AND PRIVACY, supra note 16 at 206. The sensitive private facts were defined by clause 19(1) to mean "matter relating to or purporting to relate to the health, private behaviour, home life or personal or family relationships of the individual in circumstances in which the publication is likely to cause distress, annoyance or embarrassment ..." ibid 214.

18. A.L.R.C. Report No. 12, 1979, Aust.Govt.Publishing Service, Canberra.

19. ibid, 14.

20. ibid, xi, 14.

21. ibid, xi, 16.

22. ibid, xiii, 24.

23. ibid, xiv, 44.

24. ibid, 31.

25. ibid, 6.

26. ibid, 7.

27. THE PRIVACY PROTECTION STUDY COMMISSION, REPORT, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, 1977 U.S. Govt. Printing Office, Washington D.C., 500.

28. ibid at 501 citing D.H.E.W. SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, 1973, U.S. Govt. Printing Office, Washington, 41.

29. PERSONAL PRIVACY IN AN INFORMATION SOCIETY, supra note 27, 501-2.

30. ibid, 503

31. The Data Protection Act of the Land of Hesse (Federal Republic of Germany) (Hessisches Datenschutzgesetz), 7 October 1970.

32. HONDIUS, EMERGING DATA PROTECTION IN EUROPE, 1975, North Holland Publishing Co., Amsterdam, 35. See also generally STADLEN, SURVEY OF NATIONAL DATA PROTECTION LEGISLATION 3 Computer Networks 174 (1979).

33. Wanganui Computer Centre Act 1976-7 (New Zealand).

34. The resolutions are contained in Appendix 1 and 2 in HONDIUS, 265ff.

35. HONDIUS, 69 citing COMMISSION OF THE EUROPEAN COMMUNITIES, COMMUNITY POLICY ON DATA PROCESSING, sec.(73)4300 final.

36. EUROPEAN PARLIAMENT, REPORT ON THE PROTECTION OF THE RIGHTS OF THE INDIVIDUAL IN THE FACE OF TECHNICAL DEVELOPMENTS IN DATA PROCESSING (Rapporteur, A. Bayerl) in Working Documents 1979-80, document 100/79 (4 May 1979). Hereafter referred to as the Bayerl Report.

37. ibid, 9. The resolution proposed in the report was adopted by the European Parliament. See EUROPEAN COMMUNITIES, OFFICIAL JOURNAL, 6 June 1979.

38. Published as O.E.C.D. INFORMATICS STUDY NO. 2 1971 Paris.

39. Proceedings published as O.E.C.D. INFORMATICS STUDY NO. 10, 1975, Paris.

40. HONDIUS, supra note 32, 75, 77.

41. ibid 62.

42. N.S.W. Guidelines, supra note 9, 3.

43. Resolution of the European Parliament in OFFICIAL JOURNAL

44. French Act, supra note 3, s.31.

45. Danish Private Registers Act, supra note 2, s.9(2). (Cf. Public Authorities Registers Act, loc cit, s.27(3). See also Norwegian Act of 9 June 1978 relating to Personal Data Registers (Lov om personregistre) paragraphs 6, 9, 16 and 25.

46. N.S.W. Guidelines supra note 9, 4. Cf. A.L.R.C.12, supra note 18, 18-19 concerning questions on race and religion in the Census.

47. A.L.R.C. 12, supra note 18, 9.

48. N.S.W. Guidelines, 5.

49. Resolution of the European Parliament, supra note 37, Part I, principle 2.

50. The Privacy Act of 1974, 5 U.S.C. 552(a)(e)(1).

51. 5 U.S.C. 552(a)(e)(2).

52. ibid, preamble 2 (b).

53. Canadian Human Rights Act 1977, s.56(2).

54. French Act, supra note 3, s.25. See also Austrian Data Protection Act (Datenschutzgestz), 18 October 1978, s.9(1) and the Federal Data Protection Act of the Federal Republic of Germany (Bundesdatenschutzgesetz), 27 January 1977, s.23.

55. French Act, supra note 3, s.30.

56. COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON DATA PROTECTION, DRAFT CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, Adopted by the Committee of Experts on Data Protection, Strasbourg, 25 May 1979. Published in Transnational Data Report Supplement, Vol. 2, No. 3, 16 (1979). See Articles 5(c) and (d).

57. Resolution of the European Parliament, supra note 37, Part I, principle 2.

58. N.S.W. Privacy Guidelines, supra note 9, 8-9. See also A.L.R.C. 12, 9.

59. The Privacy Act of 1974, 5 U.S.C. 552(a)(e)(5) and (6)).

60. French Act, supra note 3, s.36. See also s.37.

61. Federal German Data Protection Act, supra note 54.

62. See also for example Danish Private Registers Act, supra note 2, s.5(2); Public Authorities Registers Act, ss.9(3) and 11, and the Norwegian Act, supra note 45, para 8.

63. Council of Europe Draft Convention, supra note 56, Article 5(b).

64. Resolution of the European Parliament, supra note 37, Part I, principle 6.

65. A.L.R.C.12, supra note 18, 9.

66. N.S.W. Guidelines, 5-6.

67. See also Federal German Data Protection Act, supra note 54, s.27(3).

68. The Privacy Act of 1974, preamble to (b)(2).

69. 5 U.S.C. 552(a)(e)(c).

70. THE LAW REFORM COMMISSION, MEDICAL RECORDS, Research Paper No. 7, 1979.

71. N.S.W. Guidelines, 11.

72. Income Tax Assessment Act 1936 (Aust.) s.264. Cf. Social Services Act 1947 (Aust.) s.141.

73. Austrian Data Protection Act, supra note 54. s.18(1).

74. French Act, supra note 3, s.43.

75. 5 U.S.C. 552(a)(b).

76. A.L.R.C.12, supra note 18, 9.

77. N.S.W. Guidelines, supra note 9, 10.

78. Austrian Data Protection law, supra note 54, s.1(1).

79. French Act, supra note 3, s.29.

80. 5 U.S.C. 552(a)(e).

81. Federal German Data Protection Act, supra note 54, s.47.

82. N.S.W. Guidelines, supra note 9, 15.

83. 5 U.S.C. 552(a).

84. Canadian Human Rights Act 1977, ss.51, 56.

85. Federal German Data Protection Act, supra note 54, s.19(4).

86. Austrian Data Protection Act, supra note 54, s.47.

87. Resolution of the European Parliament, supra note 37, Part I, principle 2.

88. Ministerial statement of the Census of Population and Housing for 1981 by Mr. J.W. Howard (Federal Treasurer), COMMONWEALTH PARLIAMENTARY DEBATES (HOUSE OF REPRESENTATIVES) (AUST.) 20 November 1979, 3183, 3184.

89. N.S.W. Guidelines, 10.

90. 5 U.S.C. 552(a)(1)(c).

91. See also Federal German Data Protection Act, supra note 54, s.36(1).

92. Resolution of the European Parliament, supra note 37, Part I, principle 3.

93. Swedish Data Act, supra note 2, s.1.

94. See s.17.

95. Federal German Data Protection Act, supra note 54, s.28.

96. ibid, s.29.

97. ibid, s.5(2).

98. Austrian Data Protection Act, supra note 54, s.20(2).

99. ibid, s.20(4).

100. Resolution of the European Parliament, supra note 37, Part II, principle 8.

101. A.L.R.C.12, supra note 18, 31.

102. ibid.

103. 5 U.S.C. 552(a).

104. ibid.

105. Canadian Human Rights Act 1977, s.52(1). See also s.62(1)(b).

106. French Act, supra note 3, s.34.

107. ibid, s.35.

108. ibid, s.36.

109. Federal German Data Protection Act, supra note 54, s.4.

110. For example, the extent to which privacy regulation should be restricted to automated records or should extent to manual records; the extent to which privacy protection should extend to legal persons (corporations and associations) or should be confined to physical or natural persons; the extent to which "basic rules" of privacy protection should be confined to high level objectives as distinct from machinery questions of implementation which may be necessary for effective privacy protection; and the difficulty of distinguishing, in the context of impediments to trans border data flows, those limitations based on privacy interests and those based on other national concerns viz. trade, employment, culture, national sovereignty and so on.