354

COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

1ST SESSION, PARIS, 27 SEPTEMBER, 1982

LEGAL ASPECTS OF INFORMATION TECHNOLOGY

The Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission.
Formerly Chairman of the Expert Group on Trans Border Data Barriers
and the Protection of Privacy

The opinions expressed in this paper are those of the author and do not necessarily reflect those of the Organisation or the Australian Government.

TABLE OF CONTENTS

	Para.	Page
INFORMATION TECHNOLOGY IN CONTEXT		
A future for futurologists	1-3	1-2
Reservations	4	2
Now is the Hour	5-6	3-4
Starting without definitions	7	5
PRIVACY PROTECTION		
OECD Guidelines	8-9	6-7
Towards enforceable rules	10-13	7-9
Future Privacy Issues	14	9-11
FREEDOM OF INFORMATION		
Currency of democracy	15-16	11-12
Future Issues	17	12-14
VULNERABILITY, UNEMPLOYMENT AND CRIME		
Vulnerability	18	14-16
Unemployment	19	16
Computer crime and fraud	20	16-19
CONFLICTS, SOVEREIGNTY AND PROTECTIONISM		
Private international law	21-23	19-21
Informational Sovereignty	24-25	21-24
INTELLECTUAL PROPERTY, BUSINESS LAW, LIABILITY AND INSURANCE		
Intellectual property law	26-27	24-25
Business Law	28-31	26-27
Liability for loss and error	32-33	27-29
Insurance against computer loss	34	29
EVIDENCE LAW AND LEGAL PROFESSION		
Evidence law	35-37	30-31
Lawyers and the judiciary	38-39	31-32
INSTITUTIONAL RESPONSES		
National and international	40-41	32-33
Industry response: A proposal	42-44	33-35
OF PROFITS AND PROPHETS	45	35
ENDNOTES		36-41

LEGAL ASPECTS OF INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY IN CONTEXT

1. A future for futurologists: At the end of July 1982, there gathered in Washington a conference of thousands of business leaders, politicians, scholars and decision makers addressing the topic 'Communications and the Future'. A glance at the preliminary program issued by the Congress, and a list of even some of the hundreds of the topics addressed, indicates the complexity and the challenge of the task before the new Committee for Information, Computer and Communications Policy. It also indicates a major future for futurology. Indeed session 1401 of the Washington Congress was specifically assigned to the topic 'Career Opportunities for Futurists in the Information Society'. Just consider the variety of some of the other conference sessions, chosen, at random.[1]

* Communicating with consumers in the information age.
* New electronic information systems for finance.
* Media communication as an agent for change.
* The societal and competitive impact of new electronic banking.
* Democratic communication: bottom sideways as well as bottom up.
* The impact of advanced systems technology on future communication satellites.
* Privacy in the wired home.
* Poetry tomorrow: word art for the information age.
* Futuremoney - banking at home.
* Transferring communications technology to the Third World.
* The Yang and Yin of the communications future.
* Present shock: journalists and the new information delivery technology.
* The man-machine interface.

2. A number of issues relevant to the law and information technology were on the agenda including:

* Legal implications of home communications technology.
* Communications and the legal profession.
* Legal ramifications of communications technologies.
* Legal institutions and doctrines.
* Transborder data flow: legislative developments.

3. The variety of the topics requiring the attention of the new OECD Committee is dazzling, daunting and growing at an exponential pace. A glance at the work done and the work in progress in the Organisation, combined with speculation about future tasks, is not for the faint-hearted. Opening the High Level Conference on Information, Computer and

Communications Policies in October 1980, which gave a spur to the establishment of this new Committee, the then French Minister of Industry, André Giraud, declared that there existed no 'legal infrastructure to sustain the transition to the information economy'. The same is true to-day. It is not possible to venture, in a short paper such as this, upon a complete exposition of the design for such an infrastructure. The task of putting together that mosaic is one that must await the deliberation of expert groups, established to assist this Committee, the reports of the Council of Europe working party on information law[2] and enquiries in Member countries and beyond. Without embarking too far into the dangers of futurology, this paper will attempt to identify some of the chief legal issues that will need to be considered, particularly having regard to the likely continuing growth of transborder flows of data, with their many implications for law.

4. Reservations: At the outset, lawyerly training requires me to make a number of cautionary reservations.

* A general overview: This is no text book on computer law. For those who want to glance into the way in which computers are affecting domestic law, there are excellent general books by Colin Tapper and Peter Seipel[3]. Furthermore, extremely useful papers have been prepared for the Organisation by consultants.[4] This paper draws, in turn, upon them. It seeks to digest them for those who have tht time to grasp only the main points. The very magnitude of the social impact of informatics requires help for busy people seeking an overview from which policy judgments can fairly and accurately be made.

* Jurisdictional myopia: Every lawyer has difficulty in offering such an overview. Unlike medicine and other professions, law is traditionally locked into the culture, history, language and attitudes of its jurisdiction. In federal countries there is a further complication in the existence of laws differing as between different sub-national regions. In fact, this is part of the problem which the OECD must address. The very technology which has linked computers by telecommunications renders laws, framed in terms of power over a particular territory, inconvenient or irrelevant in many ways . The subject matter to be regulated is pervasive, ubiquitous, instantaneous. Inevitably lawyers from different traditions will approach the issues of transborder data flows (TBDF) in ways dictated by their training. Concepts will differ, institutions will differ, categories of legal reference will be different and an even greater danger will be posed where, because of history or legal tradition, the same word may conjure up quite different legal concepts because of the different way these concepts have developed. An illustration of the impact of legal traditions in this area can already be seen in the differences that

have emerged, even in a decade, between the legislative responses to the concern of privacy protection in European countries (typically generalist data protection agencies) and those found in most common law countries (typically limited and specific remedies addressing particular problems, pragmatically defined). It will be hard for lawyers and political leaders advised by lawyers to escape on the international plane from the prejudices and tendencies of their lawyerly view of the world.

Law and society intermixed: It is undesirable to see the law as something divorced from other social concerns of informatics and TBDF. The technology has economic, political and other implications, as the variety of the subjects of the OECD studies will illustrate. Indeed, the very subjects of information computer and communications policy must themselves be seen by societies and those who govern them, in the wider context of science and technology more generally. There are distinct analogies between the challenges to the capacity of political and legal institutions to cope with informatics and TBDF, on the one hand, and the equally perplexing challenges posed, on the other, by the new energy sciences (particularly nuclear fission), the new biological sciences (in vitro fertilization and genetic engineering) and robotics. The emphasis may differ. The scientist and technologist may wish to emphasise the brilliance of a new thought or the benefit to mankind of a new technology. The economist may wish to stress the international importance of maintaining free flows of data for the aggregate benefit of Member countries. The lawyer's ultimate point is more likely to be concerned with the capacity of our political and legal institutions to keep pace with the pressures of change. I am biased both by my training and by my present occupation. It will not be to the ultimate advantage of Member countries of the OECD if they expand greatly the technological advances of informatics and TBDF and yet in the process fail to solve the institutional and legal problems of providing ultimate social responses to the new technology, national and international, and addressing the legal 'fall-out'. Yet this must be done recognising that it is neither possible nor desirable to divorce legal issues from broader policy issues, even if convenience, manageability and the limitations of the human mind require us to catalogue problems and to tick off those with which we can deal. This is the practical approach being adopted by the Expert Group which is presently, within the Organisation, examining selectively and pragmatically legal questions raised by transborder data flows.[5]

5. Now is the Hour: A further preliminary point should be made. Differing views are expressed about the urgency of considering the legal problems. On the one hand, there is the opinion that delay may be beneficial because it will give home governments time to reflect and international organisations time to develop proposals.[6] On the other hand, it has been suggested by the United Nations Centre on Transnational Corporations that the

lacunae defined by M. Giraud ought to be filled promptly whilst 'important vested interests are not omnipotent and positions are not frozen'.[7] It appears from the assignment of priorities given by Member countries at the 11th session of the Working Party on ICCP in March/April 1982 that they consider legal aspects of transborder data flows to have one of the highest priorities in the ICCP program of work for 1983 Only one other matter (economic aspects of non-personal data) was voted a higher priority.[8]

6. A report by the United States Government in March 1982 listed 33 different ways in which countries could stop firms from other countries sending data into their territories, frequently by the use of domestic laws (ostensibly for privacy, copyright or other protection). The report claimed that 30 countries had already erected barriers specific to transborder data flows.[9] Whatever the number of such impediments and the present size of the problem, its existence cannot be denied. Time is not on the side of its easy solution. The problems, some of which will be listed in this paper, are such that the earlier guidelines can be offered, around which domestic laws may cluster, the better. It is precisely in work such as this that the Organisation can fulfil its most creative and influencial role. I have reason for saying this. Although Australia has not, for local constitutional and political reasons yet subscribed to the OECD Recommendation by the Council on Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, in which I had some part, the fact remains that the principles stated in those Guidelines are central to the development of Australian federal legislation on privacy protection.[10] Indeed, the Australian Freedom of Information Act, recently passed adopts, in respect of federal public sector records, the 'individual participation principle' (access to one's own file) and other principles which were amongst the basic rules for domestic application of the OECD Privacy Guidelines. So there is obvious merit, where the technology is extremely dynamic, diverse, ubiquitous, powerful and difficult or impossible to control unilaterally[11] and where the multi-faceted problems are so complex as to discourage even the most intrepid local administrator, for the OECD to offer help. Even in so peculiar and local a discipline as the law, the very technology itself creates the urgency to develop compatible laws around internationally identified guidelines. More rigorous and effective international instruments (such as treaties) may follow. But if guidelines can reduce, by their early availability, idiosyncratic and incompatible domestic legislation, that will itself be a significant contribution to the harmonisation of laws which will make the later possible adoption of enforceable treaties, so much easier and so much more likely. The unanimous support expressed by the Working Party for ICCP for the work of the Expert Group on Transborder Flows of Data, the insistence on adequate resources for the Group, the prospect of a symposium in Spring 1983, the distribution of the questionnaire addressed to legal issues, and the study of consultants' reports all indicate that we may anticipate progress. Let us hope that lawyers

and administrators can show at least a part of the same enthusiasm and dynamism, the imagination and creativity that have so marked the past two decades in the fields of information, computer and communications science and technology.[12]

7. Starting without definitions: It is usual when embarking upon a paper such as this, for the author to start with definitions. In common law countries (but not, I believe, countries of the civil law tradition) an Act of Parliament will start with a series of complex definitional propositions. Doubtless, it would be useful to attempt to distinguish between 'data' and 'information' and to define the complex collection of legal rights provided in domestic laws making up the entirety of a notion such as 'data ownership'. This will clearly be a task for those who are getting down to detail.[13] I do not propose such a course. I would, however, want, at the outset, to call attention to an important point made in the consultants' paper on 'Legal issues related to transborder data flows'. In that paper, Professor Bing and his colleagues called attention to a definitional problem of TBDF at an international level, which in domestic jurisdiction, a professional law reformer sees all the time. This is the need for law reform and development to ensure that legislation or other laws, developed in earlier times, do not, in their terms, apply unintentionally and unexpectedly to a new invention or technology. Thus, Professor Bing points out that terms such as 'telecommunications', 'broadcasting', 'information', and so on, used in international conventions developed before the rapid growth of TBDF may, in their terms, apply to some but not all transmissions of data, now and in the future. Odd results may occur. These results may be hard to justify according to any objective principle. The technology releases the movement of information from dependence upon documentation. Accordingly, definitions framed in terms of transmission of documentary matters, apt for earlier technologies of telegraphy, may now have the bizarre result of picking up and applying their rules to information transmission systems which have a teletype terminal (creating a document) yet not to a system, reproducing its essential information on a video terminal. Indeed, where both a video and teletype terminal is provided (as is often the case) the one international convention might apply to one part of the transaction, yet not to another. The illustrations given by Professor Bing and his colleagues in their paper need the attention of the world organisations which develop communications, postal and other conventions. But they also require the consideration of the OECD because, in aggregate, they may raise more general questions e.g. as to whether 'information' which we have formerly been reluctant directly to regulate in the law, may be now apt for regulation in its own right and if so the question is raised: what would be the legal, economic, political and other consequences?

PRIVACY PROTECTION

8. OECD Guidelines: It is convenient to begin the consideration of substantive legal concerns with privacy protection because this has been a sustained interest of the OECD for more than a decade. Valuable work has already been done. The history leading up to the September 1980 Recommendation of the Council is contained in the Explanatory Memorandum which accompanies the Privacy Guidelines. Although the Guidelines are not, in terms, confined to the problems of privacy and transborder flows of data in automated form, there can be little dispute that the initiating concern that led to the Guidelines and which has enhanced pressure in Member countries for privacy (or data protection and data security) laws, is the rapid penetration of computers, now linked by telecommunications.[15] Concurrent moves in the United Nations, the Council of Europe and the European Community and European Parliament are mentioned.[16] The worldwide distribution of Member countries of the OECD and the present patterns of world data flows, together with the current spate of data and privacy laws, obviously make the OECD Guidelines specially important as an international statement of accepted standards.

9. So far, only three Members have not signed the Council's Privacy Recommendation, namely Australia, Canada and Ireland. Australia's federal constitution, under which privacy (thought not telecommunications) is basically a State matter, chiefly explains the delay there. But, as I have said, the development of Australia's privacy and freedom of information laws is strongly influenced by the OECD Guidelines. In Canada, officials are very frank about the special concerns they have about the economic implications of TBDF for the Canadian workforce. But in Canada, too, there have been important developments. On 7 July 1982 a Bill enacting the Access to Information Act and the Privacy Act became law.[17] The latter adopts, as the Australian Freedom of Information Act 1982 does, the key 'individual participation principle' of the OECD Guidelines. Subject to the exceptions and machinery provisions of the Act every citizen or permanent resident of Canada 'has a right to and shall on request be given access to' personal information, as defined. The terms of the rights to request correction, annotation and notification appear entirely compatible with the OECD principles for domestic application. In the case of Ireland, it has been suggested that a change of administration may have delayed endorsement of the OECD Guidelines. For those countries which already have privacy or data laws, the Guidelines represent a standard against which they can measure their laws and in respect of which they should ensure that their laws conform. In the respect of those countries such as Australia, the United Kingdom, Ireland and elsewhere, which do not yet have privacy laws or do not have comprehensive privacy laws, the OECD Guidelines fulfil the useful task of stating the guiding principles. Furthermore let it be candidly said, they provide an impetus to action by the power of

persuasion of good international opinion.[19] The discipline provided by the recurrent necessity to respond, in this international forum, to the progress being made towards signature to and compliance with the Guidelines should not be underestimated. Though the Guidelines have no formal sanction attached either to subscription or for their enforcement in domestic jurisdiction, the discipline of explaining compliance or non-compliance is not to be under-valued.

10. Towards enforceable rules: During the preparation of the Guidelines, and in particular when the attention of the Expert Group was turned to the principles of international application, the point was frequently made, particularly by France, that guidelines, however beneficial as as educative and persuasive force, will not have self-executing authority in a court of law. Thus, as between Member countries which have signed the Guidelines, no citizen in one community could protest in the courts of another that this or that principle for the protection of personal data had not been complied with relying for proof upon the Guidelines. The Guidelines themselves provided no rules, enforceable at the behest of an individual, in whatever country. Instead, they were in the form of Recommendations addressed to Member countries, at the political level. This lacuna was constantly and properly pointed out by a number of the experts. It was recognised that to secure self-effecting laws, enforceable in domestic jurisdiction, something more than the Guidelines would be needed. Domestic laws enacting the Guidelines and in particular conferring justiciable rights upon citizens of (and possibly citizens in) other Member countries would need a future step in the development of law. The possible necessity for that future step was pointed out, when the dangers of the haemorrhage of personal information was considered, whether taking the form of the collection of personal data in a so-called 'data haven' beyond the reach of effective data laws, or otherwise. Clearly the development of a technology which virtually abolishes the tyranny of distance, the diseconomies of time and space, makes it possible and indeed likely that highly personal information will be kept on citizens of one country in data bases in another. The market for data bases expanded rapidly in the 1960's and 70's. With this expansion came the increasing collection, storage and movement of personal and other data:

> 'The market for data bases increased at a formidable rate...growing from 10,000 customers in 1965 to 2 million in 1978...The customers for these data bases came to include not only national and multi-national corporations of all types, and the financial, educational and other institutions of many countries, but also quasi-governmental organisations and governments themselves. Two classic examples which are often cited are those of the Swedish Fire Department, whose equipment is activated by a general electric data bank in Cleveland Ohio, and

the French Five Year Plan which is stored in a U.S. data bank. Another frequently cited case is that of some Eastern European airline reservation systems which are handled from computers in Georgia (U.S.)'.[20]

11. In the United States, which still has a major share of world data processing, progress has been made by the public adherence of a large number of relevant and important corporations to the Guideline principles (IBM, for example, has issued an international publication on the matter). But, without a treaty, enforceability of the Guideline principles, in the event of a dispute, would still require, in accordance with United States domestic law, the creation of a justiciable claim based upon some United States local law (statutory or common law) actionable in a court in that country. At their highest, the Guidelines could be no more than evidence of a proper, accepted standard of conduct. So we are still a long way short of unilateral or mutually enforceable international principles, let alone an international neutral tribunal to which parties with a transborder dispute about personal data can have access. The development of such an international tribunal, or the vesting of jurisdiction in an already established tribunal or the conferral of jurisdiction in international cases on domestic tribunals in accordance with settled international law will, if enforceability, actionability and justiciability are to be contemplated, depend upon a further step in the movement towards enforceable international law. This is not a reason to underestimate the value of OECD Guidelines where the technology presents an international element to the privacy complaint. It is, however, an indication of:

* the limitations of the Guidelines in domestic fora, where there is an international element in a dispute; and
* an explanation of the reason why, pending the development of such international law, countries may be tempted to react in ways that might be considered inimical to the free flow of information, in order
  ** to protect what they perceive as their legitimate interest in the privacy of their citizens and residents;
  ** to retaliate against what is seen as foreign indifference to that interest; and
  ** to ensure, at least in certain cases, that a haemorrhage of highly personal information will not occur, taking that information beyond effective local legislative control.

12. These concerns can be seen in a negative light as carrying the dangers of protectionism and impediments to free flows of data. I shall return to that concern. (See paras 24f below). But they can also be seen in a positive light. The fear that the United Kingdom might be Europe's 'privacy pariah'[21] and might lose (as it already in part has lost) economically profitable data processing because of the absence of adequate guarantees in the form of privacy or data protection laws[22] appears to have been one of the two principal reasons for the United Kingdom Government's proposed legislation on privacy protection announced in April 1982. The other was the human rights concern.[23] The coincidence of economic advantage and human rights protection is a happy and in some ways an unusual one. It is likely to continue within and between Member countries of the OECD and to provide a continuing impetus to the pressure for mutuality.

13. Most Member countries of the OECD now either have domestic privacy (data protection and data security) laws or are in the process of developing them. The scope of their application varies from general legislation to highly specific approaches, as has already been said. The machinery for enforcement varies in accordance with local institutions, traditions and practices. The inclusion of references to the privacy of legal persons or specific mention of application to TBDF also varies. The extent to which the legislation is specific to communications and information technology or addressed in more general terms to the sensitivity of data, in whatever form, also differs from one country to another. But the serious concern about this social aspect of the new technology is common. And the similarities to be found in the legislation as enacted are more striking than the differences. This is a matter for satisfaction, particularly when the desirability of compatibility of laws regulating a common technology is borne in mind. Above all, the adoption of the 'golden rule' - the right of access - is common to virtually all of the legislation so far enacted. This in itself provides pressure upon those jurisdictions which have not yet enacted laws, to do so and to do so in a form which compatibly complies with the OECD Guidelines.

14. Future Privacy Issues: The literature shows that certain matters stand out as issues for future consideration in the privacy protection debate. These include:

* Legal Persons: The extent to which privacy protection should extend to legal, as distinct from natural persons. To what extent is it apt to talk of the human rights of a statutory creation, such as a corporation, or of an association, club, partnership or small business? Obviously, this issue has political, economic and other implications. Fears are expressed that if a corporation had to disclose, identifiable information about legal persons, it might be forced into the disclosure of research data on a rival but smaller or competing corporation, association, firm and so on.[24]

Already the data protection laws of a number of European countries[25] extend privacy protection to legal persons to permit them to inspect data.[26] A paper specific to this subject has been prepared on the legal person issue. I will do no more than refer to it.[27]

* Code of Ethics: A significant development reported by the Secretariat to the Working Paper on ICCP was the decision of the Council of Europe at a recent meeting to initiate work on the development of a code of ethics for computer professionals. In most Member countries computer associations and organisations have sprung up and have established codes of ethics and professional conduct. However, such is the speed of the development of this new profession, that all too frequently sanctions are inadequate. Commonality is rare, so that such codes of practice may not (at least without some legal support) be very effective. This is not to dispute the value of developing such codes. They can fill in the gaps of general legislation. They can 'fine tune' matters of detail. They can allow for greater participatory self-regulation. Furthermore, they may be effective at the 'work face' because drawn and understood by informatics professionals rather than by lawyers.

* Privatisation: In a number of Member countries consideration is being given to the privatisation of telecommunications and a relaxation of the former government monopoly. In part, the pressure for this change is political and economic. But in part it may be attributed to the very variety and dynamism of the technology and the feeling that the private sector will be more effective in developing it than governmental agencies would be. But in the past, the government monopoly and domestic secrecy laws may have contributed, in practice, to the protection of the privacy and confidentiality of information passing through the telecommunications system including in international flows. The implications of privatisation may need to be considered, including for the privacy of data subjects.[28]

* Model Contracts: Pending the development of binding international obligations, consideration may be given to interpartes obligations assumed by contract. In order to define legal rights and duties in the event of a dispute, the forum for dispute resolution and the law according to which the matter will be resolved, there is likely to be an increasingly urgent move towards the inclusion of contractual terms in informatics dealings with an international element. A high priority has been attached to the identification of the problems arising in data processing, oriented towards the provision of model clauses for inclusion in international contracts between information providers and recipients. Professor Bing and his colleagues have suggested that short form provisions might be developed, such as 'fob' and 'cif', in order to incorporate, by a short form phrase, well understood standard contractual terms ('incoterms').[29]

14. Enhancing access: Amendments proposed to Swedish law in March 1982 address the need to improve the right of access by citizens to public documents which have been automated. The right to handle terminals and other technical equipment is dealt with, as is the anonymity of the citizen when accessing public documents. These proposals have implications for FOI as well as privacy laws.[30] The Swedish Data Policy Bill is also of interest, containing as it does guidelines and principles for the development of a co-ordinated national data policy.

FREEDOM OF INFORMATION

15. Currency of democracy: Information has been described as the currency of democracy. The sword of democracy, it is said, is blunted by the indifferent voter who is ignorant about what is going on in his country. The conventional argument for freedom of information (FOI) is that without it an informed public and real, political accountability is illusory.[31] Translating these fine principles into enforceable legal rights is not always easy; but much progress has been made in Member countries in the past decade, following the earlier examples of Sweden and the United States. Opposition comes from many quarters. Resolute government is said to require Cabinet secrecy. Public servants are said to require unreportable frankness of communications with Ministers. Federal constitutions are said to require unaccessible exchanges between the political units.[32] However, the demonstrated utility of FOI in some Member countries[33] and the realisation that government has now grown too big for parliaments always to be effective watchdogs[34] has encouraged various new forms of control, the most dynamic of which is FOI legislation. Transnational Data Report, compulsory reading for anyone in this field, regularly reports upon the gradual progress towards effective FOI legislation in Member countries. The International Freedom of Information Institute official bulletin discloses the present legislative developments. A table, reproduced from the January 1982 issue, gives the picture at that time.[35]

Freedom of Information – Status of Legislation January 1982

Country	*Study*	*Report*	*Bill in Parliament*	*Date of First Law*	*Personal Data Access Law*	*Documer Publicity Law*
Australia				1982[2]	X	
Austria				1974	×	×
Canada				1982[2]	×	
Denmark		×[1]		1970	×	
Finland				1951		
France				1978	×	×
Germany (FR)					×	
Ireland						
Japan		×				
Luxembourg				1979	×	
Netherlands				1979		
New Zealand			×			
Norway				1970	×	
Sweden				1776	×	
Switzerland			×			
United Kingdom		×				

16. Since January 1982 progress has been made in at least two countries. In Australia, the Freedom of Information Act 1982 was passed and is now expected to come into operation on 1 December 1982. The commencement date has been twice postponed to allow full public service briefings and the completion of a detailed series of seminars being held throughout the country for instruction of the Federal administration in the new regime of openness. Shortly after the Australian legislation was passed, the Canadian Act became law in July 1982. In New Zealand the final report of the Committee on Official Information (the Danks Committee) was published in January 1982. Debate is proceeding about the form of legislation. In two of the six Australian States, FOI legislation has been promised. Internationally, then, FOI is 'alive and well and kicking'.[36] In addition to general FOI legislation, enhanced means of access to government information has been provided by the development of new administrative bodies (such as the world-wide success of the Ombudsman idea) or the increase of the powers of individuals to seek and obtain reasons for administrative decisions.[37] It seems likely that a statutory right to reasons will spread, complementing the moves of an administrative kind towards greater openness. The aggregate impact of FOI legislation is designed to address the political problem posed in the aphorism 'The government did not tell because it was not asked; it was not asked because what was going on was not known'.

17. Future Issues: Apart from examination of the way in which the vehicles for greater access to public information continue to develop (whether FOI laws, appointment of Ombudsmen, new powers to administrative tribunals or statutory rights to reasons) it seems likely that a number of future developments in this area will need to be watched:

* Documents and data: Professor Bing and his colleagues point out that FOI legislation is normally framed in terms of access to 'documents'. True it is, the later laws define 'documents' widely to include information in microform or electronic form. The advent of the computer poses for some laws the difficult question as to whether computer data is, or always is, a disclosable 'document'.[38] The rapid transfer of information to computerised format will increase the urgency and importance of considering 'the principle of granting the public a right to use the equipment'.[39] As has been mentioned, proposed legislation in Sweden is already addressing this problem. As generations of citizens in Member countries become versatile in the use of information technology, it seems unlikely that they will be content to allow others to interrogate data bases for the desired public information. This consideration will give rise to new needs:
  ** to prevent unreasonable or excessively expensive access;
  ** to prevent wrongful interference in or erasure of the data base;

** to present access to data which is legitimately secret, confidential, private or otherwise not accessible; and

** to permit the record keeper to judge accessibility, to assert exemption from accessibility or to enforce deletions, protective of social values which compete with the value of open administration. In short, it will be difficult to reconcile free access by individuals to data bases with the legal machinery typically in place, most of which has been designed upon an assumption of a tangible document which may be scrutinised and evaluated by an intermediary against the claim to access and the statutory exemptions.

* FOI interaction: The passage of FOI legislation in different countries, in different terms, with different exemptions and different machinery of evaluation can give rise to legal problems because of the general indifference to these restrictions of the new information technology. Professor Bing's report details the conviction for espionage of a Norwegian social researcher who published certain findings on NATO defence arrangements which were contained in documents restricted under Norwegian law. The documents had been retrieved on-line pursuant to the United States Freedom of Information Act.[40] Similar examples abound in Member countries. In Australia, documents on defence matters which are not accessible in Australia and would not be accessible under the new FOI law, have been secured without impediment in the United States. In Japan a civil action was brought against makers and distributors of an antibiotic alleged to have caused a blood disease. Prior to bringing the suit, the plaintiff requested the Japanese Health Ministry to provide information disclosed to it at the time it licensed the use of the drug. The Japanese Ministry refused. The Japanese plaintiff obtained the selfsame information from the Food and Drug Administration in the United States because the Freedom of Information Act of that country was available to foreign requestors.[41] The new element is provided by the new technology. What may be inaccessible, even impermissable or strictly punishable in one country may be readily accessed elsewhere, or even in that country, by use of the FOI law of another country. The moral is that the new information technology is likely to hasten the influence of openness of administration under FOI laws, for the simple reason that it is rendered so much more difficult to contain the haemorrhage of information once its disclosure is permitted in one place.

* Data ownership: As has been said, most FOI legislation, untrue to its title, is framed in terms of access to documents (however defined) rather than access to information. Despite this, questions have arisen concerning a proposed legal principle of ownership of information or 'data ownership'. Copyright laws do provide

certain proprietary rights which are being extended, in some countries, to cover computer software. Mr. Peter Robinson (Canada) has expressed reservations about the notion of 'legal title to data'.

> 'It has been suggested in the United States, for example, that individuals should "own" data pertaining to themselves stored in certain systems (an electronic funds transfer data base, for example). Such an approach, particularly if extended, could create major problems in implementing and maintaining systems containing personal data. And in a bankruptcy case, could data be seized and access to it be withheld? If data cannot be 'owned' can data be 'sold', 'purchased' or 'traded'?[42]

Proponents of data ownership assert that to enforce effective control over the flow of information which now proliferates about all corporations and individuals, ultimate legal control over that information may be necessary. The fact that the valuable resource is not in an identifiable, tangible form should not, according to this view, prevent legal ownership. But whether 'ownership' is attributed to the data subject seems less important than that enforceable legal rights should be defined which effectively protect the interests of the data subject in information circulating about himself.

* Private sector: So far, FOI has been overwhelmingly a public sector debate. Private sector organisations are generally roped in to the extent only that they have dealings with agencies of government. It seems likely to me that the development of greater openness of administration will not be confined to the public sector but will gradually extend into the private sector as well. Domestic legislation already enforces a degree of openness to shareholders and consumers. It seems probable to me that the principles of accountability will go further, encouraged by the dynamic of the new information technology itself for this makes access to data (and hence information) quicker, easier and cheaper than it was in the past.

VULNERABILITY, UNEMPLOYMENT AND CRIME

18. Vulnerability: Just as Sweden led the way with FOI and privacy (data protection and data security) laws, now it is providing a stimulus to Member countries and to the Organisation with its detailed consideration of the greater vulnerability of the 'wired society'.[43] To institutionalise consideration of the dangers to orderly society and the concentration and distribution of information by informatics and TBDF, a Vulnerability Board was appointed by the Swedish Government in July 1981 as an advisory and consultative body concerned with security and vulnerability in relation to automated data

both in the public and private sectors.[44] A plan of action submitted by the Board examines 'vulnerability factors' and criticises the penetration of society by informatics, which has occurred without adequate resources being assigned for the increased security and vulnerability problems that are the result. 'Vulnerability', it concludes, is 'unacceptably high'. In part, the response proposed is the raising of political, business and community consciousness and knowledge about the dangers, so that they will be recognised and addressed voluntarily. In part, the problems are of such a nature that new laws will be required. The plan of action formulated by the Swedish Vulnerability Board specifically addresses the TBDF issue by listing dependence on foreign countries for spare parts, maintainence, data processing and otherwise as one aspect of vulnerability which results from the new technology. But even confined to domestic jurisdiction, a number of concerns have been identified. They include:

* methods for testing vulnerability;
* staff related factors (dependence on key-staff, training, computer crime and labour market aspects);
* concentration of service centre operations;
* destruction of ADP files;
* ADP in wartime.

It was pointed out in the earlier Swedish report that peaceful and lawful government of a computerised society is more susceptible to damage as a result of terrorism, industrial action, or simple accidents disrupting the inter-connections between data bases. These transmit much more information, vital to the economy and orderly life, than was possible before the advent of informatics. There seems little doubt that this increased vulnerability will give rise to the need for new laws, some of them containing increased coercive powers for the protection of society against the greatly increased risk of widespread damage that may flow from interference in the information technology. The special balance struck in Member countries between law enforcement and individual liberties will come under challenge as a result of the perceived risks that will arise from the dependence on the new technology. Although high priority has not been assigned to this issue at this stage, and although major disasters have not yet come to light, it does not require much imagination to see that disproportionate dislocation could be done to orderly government, economic stability, transport arrangements and domestic tranquility by destruction, loss or erasure of automated information. The protections that existed in the diffusion of information in earlier times has been lost. Attention will need to be paid to traditional freedoms in designing laws for security, protection and retaliation.

19. Unemployment: A linked concern is the effect of persistent unemployment on domestic tranquility and peaceful government. There is no doubt that the advent of new information technology has promoted fears of loss of employment in aggregate and loss of employment to 'data rich' countries[45] in particular. So far as loss in aggregate is concerned, this is one of the concerns before the Ad Hoc Expert Meeting on Information Technology, Productivity, Employment and Working Conditions on 2-3 September 1982. The introduction of information technology and robots in industries, particularly in the United States, Japan, Eastern and Western Europe inevitably has implications for employment. The meeting of the Working Party on ICCP in March/April 1982 expressed its continued high interest in what it termed the 'problem area' of information technology, productivity and employment.[46] There is no doubt that in virtually every Member country there is concern about the erosion of respect for institutions, including the law, that could attend endemic high levels of unemployment, unless these could in turn be addressed in a constructive way. The increase in petty crime that accompanies high levels of unemployment, the despair of people, especially young people, surrounded by wealth they cannot hope to attain, and the special problems of dealing with more people dependent on social security benefits are just some of the features that accompany serious and prolonged economic downturn. When the downturn is accompanied by structural change and rapid technological change displacing employment, the potential for widespread unlawfulness and erosion of authority is very considerable indeed. The technological and economic consequences of these developments are being considered in the Organisation. But it is also important that the social, legal and institutional implications should also have a due measure of consideration.

20. Computer crime and fraud: One aspect of the greater vulnerability of the wired society is its greater susceptibility to damaging anti-social conduct, such as computer terrorism and computer crime. There are many issues here for the law and its personnel in Member countries.

** Crime is strictly defined: The manipulation of information technology to steal money from a bank or property from an owner may not come within the present definition of 'theft' contained in the law. In the United States, court decisions have held that theft of a program contained in a computer's memory could not be regarded as theft of an 'article' within the scope of the definition of crime contained in the relevant statute.[47] Offences designed and described before the advent of informatics may not, in terms, apply to the conduct which now occurs. Although admittedly anti-social and harmful, unless the conduct fits within the current penal classifications, there may be no effective way of bringing the conduct to criminal punishment. In the United States the implications of TBDF in the context of computer crime were considered in the United States v. Seidlitz.[48] In that case Berthram E. Seidlitz was charged with violating

the federal interstate transportation of stolen property statute. However, he was acquitted because it was held that the only thing that had crossed state lines was a series of impulses over telephone wires. It was suggested that such a transient impulse was not within the comtemplation of 'interstate transportation' or 'property'. Similarly, there are reports of a recent case in Canada:

> 'An individual was accused and convicted of illegal use of telecommunications facilities, when in fact he had used a terminal to obtain unauthorised access to a university computer. On appeal to the Supreme Court [of Canada] the conviction was quashed and one of the Supreme Court Justices in his judgment said, in effect, that if Parliament had felt that an unauthorised access to a computer should be punished, it would have passed an appropriate law. But if the mere act of copying data becomes a crime, where does that lead us in regard to the millions of copying machines now spread around the world?...The Canadian Government has come to the conclusion that the Criminal Code does in fact need revising and is now taking steps to do this'.[49]

** Crime is local: A complication that emerges from a ubiquitous and international technology in its application to crime is the general principle, recognised in international law, that crime is local in the sense that domestic courts are normally confined to punishing criminal offences which occur in their own territorial boundaries or which have some other relevant connection with that territory. The scope of the 'relevant connection' is constantly being scrutinised by the courts and it is sometimes enhanced. In R. v. El-Hakkaoui [50] the English Court of Appeal had to deal with the case of the jurisdiction of an English court in respect of an alleged conspiracy by the defendant to contravene an English firearms law but in respect of a victim who was outside England. In fact, the defendant had intended to use firearms, discovered in a search at Heathrow Airport, to kidnap French government officers in Paris with a view to procuring the release by the Government of Morocco of a number of political prisoners. It was held that there was no rule of comity to prevent the United Kingdom Parliament from prohibiting, under pain of criminal punishment, persons present in the United Kingdom, and so owing local obedience to the law, from doing physical acts in England, notwithstanding that the consequences of those acts were to take effect outside the United Kingdom.[51] Similarly in the Stonehouse case, the English House of Lords had to deal with the converse problem of an attempt outside the United Kingdom jurisdiction to commit a crime within the jurisdiction and whether this was within the power of the English courts. In mid 1974, Mr. John Stonehouse had his wife take out 5 insurance policies on his life. He

also procured two false passports. On a trip to Miami he staged a disappearance whilst swimming. As was intended, the news was quickly transmitted to England by the media. His wife, ignorant of the deception, had made no claims on the policies when Stonehouse was discovered in Australia, although some enquiries have been made by solicitors. The issue was whether the English courts had jurisdiction over the offence of attempting to obtain property by deception contrary to the Theft Act although 'the final act alleged to constitute the offence of attempt had occurred outside the jurisdiction'. The House of Lords unanimously dismissed Stonehouse's appeal. Lord Edmund-Davies said:

> 'The law must keep in step with technical advances in international communications and the dissemination of news, and one who has it in mind that they will be utilised by others and, indeed, banks in their doing so must, in my judgment, be treated no differently from one who himself posts a letter or telephones a message or makes a personal broadcast, in which events learned counsel accepted that the issue of justiciability could not be in doubt'.[52]

At the very least, it would appear clear that, where crimes are constituted of a number of elements, some of which may take place outside domestic jurisdiction by reason of access to international data communications, reform may be needed to ensure that the legitimate jurisdiction of local courts is not improperly frustrated by technical arguments based upon the principle of the comity of nations which confines the criminal law, as an exercise of sovereign power, substantially to the sovereign's territory. The problem may be as much one for the sub-national divisions of a federation, as it is for a sequence of events which occur, in part in different countries.[53]

** Computer crime is unmeasured: One of the difficulties of the Organisation is that of estimating the extent to which and the direction in which Member countries have moved to deal specifically with crime involving the use of information technology. Sweden alone appears to have national statistics which distinguish 'computer crime' from other crime. A short questionnaire is now being distributed to Member countries concerning computer crime legislation and a meeting of experts concerning the subject is under consideration, following the analysis of the responses. It may be that this will lead on to a check list of vulnerability and computer crime issues to be addressed by Member States. The need for a degree of mutuality and reciprocity is promoted by the technology, which is not confined to one jurisdiction or territory but, on the contrary, may be instantaneously available in very large numbers of territories, in any number of which different elements constituting the crime may occur.

New crimes/personnel are needed: If data cannot be 'owned' or if otherwise it falls outside the characterisation of theft, fraud and other crimes as presently defined, it may be necessary to develop a new definition of the anti-social conduct of deliberate intrusion into the legitimate rights of suppliers and users of data. If unauthorised access to and copying of data does not of itself deprive the legitimate users of their own access and use, but nonetheless is wrongful and does harm to the users and to society, is it sufficient to rely upon any civil law remedies or may it not be necessary to develop a new criminal law concept? Jan Freese (Sweden) has proposed such a new concept in the notion of punishable 'data trespass'. Even assuming that the definition of new crimes and the complication of the international elements of information crimes could be satisfactorily overcome, it is fairly clear that serious problems exist in recognising, detecting, proving and punishing such crimes. Some initiatives are being taken by Interpol to train police in the new problems of policing the world information society. But the potential of the computer criminal to evade detection and capture, let alone trial and conviction, is enhanced by the ubiquity and universality of some of the more vulnerable information systems, such as those dealing with banking, insurance and credit information. If effective and highly skilled policing is to be developed, it seems likely that international co-operation in policing will have to be strengthened and enhanced, if only to reflect the international character of the vulnerable object of new international crime.

CONFLICTS, SOVEREIGNTY AND PROTECTIONISM

21. Private international law: The sudden development of a new technology with the features of the new information technology presents novel challenges to private international law. This was recognised by the Expert Group which developed the Guidelines governing the protection of privacy and transborder flows of personal data. In the Explanatory Memorandum, accompanying the Guidelines a central aspect of the problem was described thus:

> 'As regards the question of choice of law one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. That is particularly difficult in the case of international computer networks where, because of dispersed locations and rapid movement of data, and geographically dispersed data processing activity, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied'.[54]

In the context of personal data protection the suggestion advanced was that preference might be given to domestic law offering the 'best protection of personal data'. It was acknowledged that this could lead to solutions which were too uncertain, including for data controllers.[55] It was for that reason that, in the context of international co-operation, the Guidelines are confined to an exhortatory observation:

> 'Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data'.[56]

22. The problems identified in connection with personal data are perhaps more acute in relation to the rapidly growing numbers of information transactions of a commercial character having nothing to do with personal data but perhaps more likely to give rise to legal disputes. The kinds of doubts and uncertainties about the forum, applicable law and remedies available where a transaction has an international component are potentially multiplied many times over. This is because of the diffusion and coincidence of the potential international components in a transaction utilising the new information technology. This point was made by Mr. William L. Fishman before the United States Senate Banking Committee on International Finance and Monetary Policy in November 1981 when he urged closer attention to the legal implications of TBDF:

> 'When an electronic message is generated in country A, switched in country B and C, transits country E, F, G and H, processed in country I and J, stored in country K and involves entities residing in or operating in yet other countries, it is debatable whether existing choice of law and conflict of law doctrines are adequate. What law applies to data processing carried out by computer aboard a synchronous orbit satellite? Do we need new forms of remedy for information theft, for information mishandling? Do we need new rules on commercial entities' information rights and obligations? New fora in which to prosecute these matters? New law making institutions? If so, how do we get there? Bilateral arrangements; multilateral arrangements; private contract law; world conference? I do not know the answers; I know other countries are studying these questions and I know the U.S. is not, either in government or in the private sector'.[57]

In a June 1980 statement by the United States Delegation on the legal issues in transborder data flows, potential solutions for TBDF conflicts were listed. Those mentioned included applying the law of the State of the data subject, of the data controller, of the State of primary processing and data storage, of the State where decisions were taken on the basis of the data, the law of the State of beneficial user or the imposition of an entirely new international substantive or procedural law specially designed for the purpose.[58]

23. How are these choices to be made? How is a regime to be developed for the technology which is so rapidly penetrating all of our countries? How will we authoritatively and finally determine the problems of fora, choice of law, procedures and remedies identified by the above statements?[59] The United States statement suggested that the OECD might not be the appropriate forum in which to approach all of the mixed issues of law, economics and policy. The Hague Conference on Private International Law has specialised over many years in studying conflict of laws questions. It has 29 members including many European countries, the United States, Canada, Japan and Australia. Hague Conventions typically apply only to the international sale of goods. Consequently, in terms they may have has no application to trade in computer services. Professor Bing and his colleagues consider that drafting an international convention is a long term project[60] and that in the meantime it would be desirable to encourage the development of guidelines and of standard contractual clauses such as have already been mentioned.[61] However, until binding conventions are developed, there is a danger that municipal courts will go their different directions. The complexity of the technology for lawyers, not normally comfortable in the world of technology, will invite confusion in legal decisions, and conflicting and competing decisions in different countries regarding the same transaction, unless authoritative and internationally agreed principles can quickly and conclusively be settled. The resolution of the OECD Council establishing the Committee for Information Computer and Communications Policy includes an instruction to 'take into account the work of other international organisations active in the field of information, computer and communications policy'.[62] Clearly, the Hague Conference is one such body. In my view an active and mutually supportive liaison should be established without delay.

24. Informational Sovereignty: In the same statement by Mr. Fishman to the United States Senate Sub-committee it was pointed out that the legal concept of 'sovereignty' was possibly undergoing a change:

> 'The rapid development of international telecommunications in the past 25 years and the enormous development of data processing technology has assured that all

developed economies are inter-related in a thousand taken-for-granted-ways...Multi-national activity is the backbone of the Western economies; telecommunications and data processing are the backbone of multi-national activity...Many other countries, developed and Third World, east and west, began to recognise a few years ago that the international economy was information based; a large number of foreign governments determine that sovereignty in an information age was no longer simply a matter of physical borders and political allegiance, but instead was evolving toward access to, control over and reliance on information resources. How, these nations ask, could they be sovereign, when their economic, industrial, perhaps even academic and social lives were dependent upon foreign-based information resources? While I would not characterise these concerns as universally anti-American, it was widely (and correctly) recognised that the U.S., through capital investment, risk taking, economies of scale and sheer entrepreneurial energy had captured a very large proportion of world markets in information goods and services. Having identified information resources as the key to the future, and having identified what was perceived to be foreign domination, many countries have set out to assert their independence, both political and industrial, in this growing field'.[63]

25. The issue of sovereignty and informatics is complex and, from the legal point of view, has a number of aspects:

* Vulnerability: The first is linked to the issue of vulnerability. One United States journal suggested that the freezing by the United States during the illegal detention of hostages in Iran, of the assets of Iran 'fuelled the apprehension' of some countries concerning the extent to which data, essential to their national economies, is stored in the United States. The same point could perhaps be made in relation to recent United Kingdom and European retaliation against Argentina. In the past, seizure of enemy assets was a personal tragedy and a national inconvenience. But it did not hold the same potential for widespread disruption that would arise if a country had effective control over the storage, processing or transit of data vital to an enemy. Concern about this potential for political or economic 'leverage' has doubtless produced or encouraged development of laws, or the application of earlier laws, to limit what is seen as the loss of an important attribute of sovereignty. This is the control over vital national resources. A list, conceded to be incomplete, of the potential problem areas would include:

* restrictions on import of data processing systems;
* restrictions on export of information;
* restrictions on use of international telecommunications channels;
* domestic industry subsidies;
* export or import tax on information;
* buy national policies;
* taxes on automation of plants or offices;
* restrictions on access to foreign data banks.[64]

The issue is not entirely theoretical. Brazil, perhaps more than any other country, has designed a full set of policies to deal with TBDF. Its efforts grew out of a national computer policy which aims at facilitating the creation of national capabilities. Since 1972 a federal agency has supervised the use and acquisition of computers first for the federal government and since 1976 for all computer or computer parts used in Brazil. In 1978 legislation required that all transnational computer communications systems should become subject to the approval of the agency. Between 1978 and 1980, 19 applications were filed and decisions were taken on 16. Approval was denied for applications related to the use of time-sharing services and data banks abroad, and to certain types of international operations of foreign affiliates. Approval was given for airline reservation systems and demonstration systems. Putting it generally, the government of Brazil 'does not allow the use of computers placed abroad which through teleinformatics would accomplish tasks whose solutions could be obtained in the country.[65] The Brazilian action, and the prospect of its being copied elsewhere, led some journalists to coin the notion of a 'world data war'.[66] The United States was described as the 'OPEC of information'. On the other hand, in the United States, legislation was proposed in retaliation to give that country 'leverage'.[67] The Brazilian law and the suggested misuse of privacy laws in other countries, may be seen by some as an unacceptable interference in the free flow of information. Others, looking at the same issue from the viewpoint of their own national interests, may see the legal developments as nothing more than an assertion of old-fashioned features of national sovereignty in a world where the problem has changed with the advent of new information technology.

* Is it sovereignty? Still other commentators have questioned whether it is sensible to talk of 'informational sovereignty' at all. Peter Robinson, whilst conceding that economic realities affect a country's practical freedom of action, doubts that it is helpful to express the predicament in terms of a legal notion such as 'sovereignty' which has, in international law to date, been taken to refer only to the legal powers a country has to control national policies and to exercise jurisdiction over a specific tract of territory.

'It is obvious that the political, economic and technological realities of an increasingly inter-dependent world community pose practical constraints on State behaviour but do not necessarily involve derogation of sovereignty or alter basic principles of international law'.[68]

According to this view, it is much more useful to examine hard practical problems than to indulge in theorising about vague new concepts such as 'informational sovereignty' or 'cultural sovereignty'. Accordingly, more attention should be paid to sorting out the choice of law problems and to considering the effective extra-territorial operation of domestic laws that can attend the international reticulation of information through the new technology. If this view were taken, there would be a number of legal questions to be examined, associated with the dangers of legal protectionism. Some of them are identified in the paper by Professor Bing and his associates. They include principles proposed to be adapted from earlier treaties designed for the movement of goods. Only some of these will survive the translation into the dynamic, instantaneous technology of information. Principles such as the prohibition of dumping, the right of innocent transit, the right of custom-free transit, of the determination of title and so on all deserve careful attention.[69] Mr. Robinson has proposed that the Expert Group on Transborder Data Flows should concentrate on practical tasks, selected pragmatically, rather than on ideological tasks of great sensitivity such as national informational sovereignty. It would appear more likely that the latter notion, if it is to be developed, will arise in other fora, quite possibly on the initiative of countries which are 'information poor'.

INTELLECTUAL PROPERTY, BUSINESS LAW, LIABILITY AND INSURANCE

26. Intellectual property law: Traditionally, intellectual property law developed around protections which attached to the medium rather than the content. It was not possible to patent or copyright an abstract idea. Patents attached to 'inventions'. Copyright attached to the original 'work'. The law of confidence and the law of defamation attached its consequences typically to the act of unwarranted communication or publication rather than to the information itself. The problem posed by informatics technology is that data (and therefore information) have now been 'liberated' from physical objects representing the data.[70] Thus, is has become possible, technologically, to read the text of a book without purchasing the book, or even copying the text. Information technology has made information a commodity.

'There is a paradox inherent in the sale of information in that once a buyer knows exactly what he is purchasing, he has no need to purchase it, for he then has it already. Secondly, though information may be expensive to create and costly to compile, once obtained it is cheap to reproduce.'[71]

Because intellectual property law has traditionally attached itself to physical objects, representing information, the information itself has only been indirectly regulated. This approach is no longer apt for the new 'liberated' world of informatics. The difficulties are aggravated by the phenomenon of TBDF, by which information produced in one country may be reproduced in ephemeral form in another. Unless some new arrangements can be made, recompense to the original author may be readily and entirely avoided.

27. The problem of applying old notions of intellectual property law to the new medium has been recognised in the World Intellectual Property Organisation (WIPO) since at least 1967. WIPO has established an Expert Group on the Legal Protection of Computer Software. It had its first meeting in November 1979 and it is considering a model provision for the protection of computer software. A committee of government experts on copyright problems has also been established by UNESCO.[72] Cases have begun to appear in the courts arising out of the way in which TBDF can, by its ubiquity, offend the monopolising features of intellectual property law. These are features which are the reward of those who create new inventions and works. A copyright proprietor may have copyright subject to territorial limitations. If the provider offers his services internationally, the copyrighted material might, by TBDF, be retrieved by a user in a jurisdiction where another licensee holds the exclusive right to furnish copies. This use may then constitute a copyright infringement in that country.[73] In many countries, including Australia, advisory committees have been established to examine the development of intellectual property law so that it will fit more comfortably with the highly creative but ephemeral and distributive nature of the new information technology. Proprietary rights to original material are now being extended in many countries to cover computer software.[74] Clearly further substantial developments will be needed. The OECD may not be the appropriate forum in which those developments can most efficiently and expertly occur. However, as a body concerned with the economic and social implications of information flows, it will obviously be vital for the Organisation to evaluate the monopolising and protective features of intellectual property developments as they impinge upon and limit the tendency of the technology to promote free flows of information, including across borders.

28. Business law: It has been suggested that movement of goods from country to country was hampered at the time of the first industrial revolution, diminishing the potential for spreading the benefits of technology, by 'narrowly conceived national interests' which resulted in the development of municipal laws which destroyed the simplicity and uniformity of maritime and commercial law and gave rise to 'sharp conflicts of laws'.[75] Concern has been expressed that we should not make the same mistake twice. In part, this is a call for agreement upon choice of law and conflict of law principles such as have already been mentioned. But it is also, in part, a call for the identification and harmonisation of some domestic business laws and practices, so that the opportunities for inconsistency and disharmony are avoided or at least diminished.

29. Some satisfication and encouragement can be drawn from the successful establishment and expansion of closed user-group transnational computer-communication systems. These networks serve the needs of subscribers having a high level of precisely common interests. The best known systems of this kind are Eurex S.A. and the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which service the financial community and the Société Internationale pour la Télécommunication Aeronautique (SITA) which services the air transport industry. The success of these systems does not put them beyond potential domestic legal regulation. Indeed W.L. Fishman in his address to the United States Senate Sub-committee put it in this way:

> 'I have always thought that the banking industry was particularly vulnerable to the growing tendency to impose restrictions on information flows; banking is increasingly an information exchange process, particularly international banking. Banks also deal in particularly sensitive areas of national concern, including such matters as national credit standing, capital formation, currency exchange regulation, monetary and fiscal policy, personal privacy and so on'.[76]

Similar observations could be made about personal travel and hotel bookings. Mr. Fishman's concern was that the 'rosy picture' of unregulated or acceptedly regulated international data flows was not likely long to endure.[77]

30. The need of all countries having personal transactions and business contracts to have access to these international systems may inhibit too gross an interference by national laws. The greater risk may arise from the development of national laws in the pursuit of other perceived national goals which in consequence (and especially in aggregate) impinge upon TBDF in a restrictive way. This is precisely what happened in the 18th and 19th centuries with the developments of local commercial and maritime laws.

indeed, it has happened right into this century. The difficulties occasioned in getting agreement on a new Law of the Sea stand as a lesson of the problems that may face future lawmakers in resolving the complexities of a Babel of local laws once a proliferation of domestic laws has occurred, which impinge upon the international technology.

31. Of special relevance to business law will be the developments in telecommunications by which business contracts are effected. Already international transmission of contracts, bills of exchange, bills of lading, airway bills, letters of credit are occurring. The problems that arise go far beyond those of private international law which have already been mentioned. They extend beyond the choice of law to govern a contract, the choice of forum to resolve disputes and the remedies for enforcement of decisions. They include also the need to provide for mistakes, to resolve the kind of circumstances in which there has been such a meeting of minds as to constitute the mutuality of contract. They include the need to reconcile important differences in contract laws - particularly as between the approaches to contract taken in English speaking common law countries (where the doctrine of consideration reigns) and countries of the civil law tradition. The instantaneous technology speeds up the processes of negotiation in a way that earlier merchants could avoid by delay. Today's merchants work in a world of complex statutory laws governing anti-trust, taxation obligations, banking and foreigh exchange regulation, rules governing relations with administrative authorities, foreign investment limitations and so on. Instantaneous contracts may not permit adequate time for advice on the complex range of laws that affect or even destroy the contract, once made. The latest ICCP newsletter records the development of electronic mail by the German PTT.[78] It is said that international standards have now been agreed for electronic mail. But whilst these have been addressed to technological problems, most of the legal problems remain to be unravelled. This may be another area in which model provisions for inclusion in international contracts could be developed. This in turn could, according to Professor Bing's paper, possibly be drawn on the precedents of traditional transport treaties and other like international instruments. But these will not, in their current terms, generally apply because they were designed for the pre-existing world of goods and documents not for the present and future world of information, fleetingly and electronically exposed on the VDU.[79]

32. Liability for loss and error: Mistakes can occur in electronically transmitted documents, just as they can occur in contracts written on vellum in copperplate. A defamation can be fed into a data base and do great harm and hurt upon publication to the many users of the system. The occurrence of computer error is not great when compared to the enormous dependence on information technology nowadays. Yet potentially it might be catastrophic and would affect very large numbers of users. Errors can arise out of human factors (such as defective programming, inattentive keying of data,

wilful inclusion (or deletion) of data. It can also be the result of defects in computer hardware (a failed valve, loss of power, etc.) or loss or interference during transmission.[80] In a consultant's paper, reference is made to the humorous and hypothetical case of Mr. Haddock whose reputation was damaged because a lowering of voltage by an electricity board resulted in a malfunction of a bank computer. The case was written, not entirely in jest, originally in the satirical magazine Punch.[81] But the problems discussed in the article, written by A. P. Herbert nearly 20 years ago, could arise. The questions raised included the definition and scope of the liabilities of the bank, the electricity board and others eother in contract or in tort (civil wrong) or under statute. Cases in which losses have occurred as a result of what may be generally categorised as 'computer error' generally come back to a fundamental practical issue: who is to absorb the losses? Is it

* the computer hardware manufacturer or maintenance?
* The programmer?
* The employer of the officer who made a mistake or wilfully caused damage and loss?
* External parties whose conduct affected the efficient operation of the computer?
* The PTT authority responsible for transmission of the information?

33. These problems, difficult enough within a single jurisdiction with a single system of laws, become almost intolerable, where, by reason of TBDF, multiple jurisdictions with their differing legal rules may become involved. In an international industry, with international personnel servicing the international flow of data, at any point of which, error, breakdown or interference can occur, the potential for real legal problems in fixing liability for losses will be considerable. In part, the risk of loss can be excluded either by domestic legislation (such as typically protects telecommunications authorities) or by contractual terms. Difficulties may arise in the path of lawyers seeking to squeeze the conduct of programmers and the services they supply into legislation which was designed in earlier times to deal with breaches of contract for the sale of goods, breaches of warranty concerning tangible products and strict liability for physical objects.[82] However, these are not likely to prove fatal impediments in the way of lawyers arguing, at least in countries of the common law tradition, that negligent advice given by proported experts concerning a particular computer program, causing loss, will sound in compensatory damages. Similarly, the principle of vicarious liability requiring an employer to indemnify for an employee's negligence may result in very considerable losses falling upon the employing corporation or agency as a result of careless or even wilful mistakes which have a profound and widespread damaging effect. In short, although the introduction of informatics and TBDF has so far been attended by relatively few reported

cases, this should not be a reason for complacency about the potential for legal liability that can arise from human or computer error. The novelty of the technology may in part explain the lack of reported cases. The daunting complexity of establishing the technology and proving error (particularly if there is an international element in the case) may explain the disinclination to bring litigation. Exemption by legislation or contract may have prevented some cases from being launched. It seems unlikely that this position will continue. Indeed, it may be unjust for it to do so.

34. Insurance against computer loss: Insurance is about the spreading of risks which are shared by the many against the chance that some will suffer loss. Liability insurance in respect of damage resulting from computer error could be developed. To some extent, current insurance policies will already provide indemnity for errors arising out of information technology and TBDF. For example, an airline disaster caused by incorrect plotting of a flight path using a computer and TBDF may give rise to claims against the airline which is indemnified under the airline's accident liability policy. Likewise, negligence by a data processing employee or engineer causing loss may give rise to claims under professional indemnity or like insurance. The need for the development of liability insurance specific to worldwide computer systems is yet to be fully explored. But it does seem likely, on the analogy of airline insurance, that something will be needed. The losses when they occur are likely to be large and sometimes disastrous. The provision of a common insurance fund may be fairer to all who are using the system. Attention has been drawn to the system already developed in the field of accident compensation to provide no-fault entitlements to those who inevitably suffer as a consequence of the use of the motor car. In New Zealand, a most novel reform has been developed by which accidents, however caused and wherever occuring (whether at work, in a car, at home, during sport or otherwise) are compensated under a national compensation scheme. Private insurers typically resist compulsory and generally government funded insurance schemes of this kind. A proposal for a similar accident compensation scheme in Australia has not, so far, been adopted, partly because of resistence from the private insurance industry. However, if damage arises to users of a computer system, in circumstances that recovery is not possible or certain, calls may be made for the computing industry, or particular segments of it, to develop procedures for the fair allocation of risks amongst the several participants.[83] This may be especially necessary because of legislative or contractual provisions limiting or excluding liability in the case of the organisations most readily able to bear the losses that occur from high speed processing and transmission of information. It may be desirable because of the prohibitive costs and uncertainties in legal disputes having an international component, because of the use of TBDF.

EVIDENCE LAW AND LEGAL PROFESSION

35. Evidence law: A result of its historical development, and the primacy in it of jury trial, the English common law, which is the basis of the legal system in six Member countries, developed complex and highly technical rules of procedure and evidence. Indeed these are said by René David to be at the heart of the 'different character' of that system of law.[84] The emphasis upon a continuous, public and oral trial, often before a jury, has fashioned the rules which limit the admissibility of evidence in the trial. In systems of law which adhere to the common law tradition, there is a need significantly to modify the laws of evidence and to permit more readily the admissibility in court of computer evidence and computer generated evidence. The basic problem is the hearsay rule. In its original form, this rule forbids the admission at the trial of evidence, oral or documentary, which cannot be deposed to from his own knowledge by the person giving the evidence before the court. This rule, though founded in historical reasons is also grounded in principles of procedural fairness. Litigants should be able to face and test by cross-examination their accusers. Courts should base their decisions only on reliable and, where necessary, tested and scrutinised information. In the solemn business of judicial determination, particularly where the criminal law is being invoked and liberty is at stake, the means should be available to check and verify material before a court accepts and acts upon it. The advent of computing, photocopying and electronic communication and their widespread, indeed international, use render the maintenance of this hearsay rule in its original form unreasonable and indeed impossible. Clearly it would be intolerable to require that every person who had contributed to a much used and thoroughly relied upon computer record should be available to prove orally his individual contribution to the computer record. Particularly would this be unreasonable in the event of computer material originating or generated in a foreign country and transmitted, possibly across the world, by TBDF. The rule was unreasonable in the case of business records before computerisation. It becomes even more unreasonable when computerisation is employed. Yet mistakes do occur. It is simply not appropriate to accept, without any precaution or reservation the printout of every computer, as if the technology itself were an indisputable guarantee of accuracy and, in some mystical way, provided protection against false, negligent or even malicious and misleading information. An American judge undoubtedly spoke for a large constituency when he complained in a judgment that as 'one of many who had received computerised bills and letters for accounts long since paid', he was not prepared to accept the product of a computer 'as the equivalent of holy writ'.

36. What is therefore needed, in common law countries, is legislative reform to provide for the readier admission of computer evidence and computer-generated evidence without the necessity in every case of oral proof of the original source. In the United States, the most common form of legislation to deal with this topic is an elaboration of an exception to the hearsay rule adopted earlier to cope with business records of large and impersonal corporations. In England amendments to the Civil Evidence Act 1968 provide for the admission under certain circumstances of a 'statement contained in a document produced by a computer'.[85] Review of this area of the law is now being actively pursued in Australia by the Law Reform Commission. The Federal Parliament and a number of States have already adopted certain legislative reform measures.[86]

37. Although the problem of modification of the laws of evidence may, as such, be peculiar to common law countries, there is undoubtedly an analogous problem for the conduct of tribunal and court hearings in any legal system where procedural fairness requires that a party or a witness, confronted by the product of information technology, should, if it is important enough, have the opportunity to challenge and test the information. If necessary this may require getting back to its source. On the other hand, though this problem may be inconvenient for countries outside the common law world, its resolution is nowhere near as painful as it is in those [typically English-speaking] countries. The resistance to hearsay evidence, the adherence to the continuous oral trial, the persistence with the jury of ordinary citizens and the need often to bring complex technical questions back to a non-expert, generalist tribunal all present special difficulties for those brought up in the trial traditions of the common law. Between lawyers in those countries, there is a healthy exchange of information and experience. Innovations in legislative exceptions to the hearsay rule, adopted in one jurisdiction, are considered and sometimes copied in others. Although this is not a universal problem, it is a specially relevant one to Member countries of the common law.

38. Lawyers and the judiciary: The new information technology brings good and bad news for the legal profession. The good news involves the improvement in access to legal data, including the potential of readier access to overseas legal material by TBDF. A recent issue of the journal of the Law Society of England and Wales recounts the way in which transmission of legal data and funds by telecommunications will expedite the transfer of land title in Britain.[87] A Working Party of the Committee of Legal Data Processing of the Council of Europe is reported to be examining the relationship between the providors and users of legal information services in Europe. As reported, the examination includes consideration of the issue of liability when errors in the data base cause economic loss for the user.[88] Most Member countries have established or are in the process of establishing on line legal data bases. The electronic law firm is fast becoming a reality in all Member countries. Word processors have taken over the routine

of much legal activity. They carry the potential for cost savings that may bring more people more readily and economically to justice. One New Zealand commentator has suggested that an urgent obligation of lawyers is to simplify old precedents before they are immortalised and mass produced through word processor technology and transmitted widely through telecommunications.

39. The bad news may not be universal. But it certainly affects a number of countries where the staple activity of the domestic legal profession is concerned with land title transfers. In Australia, for example, approximately 50% of the fee income of lawyers, scattered over the face of the country, is derived from this activity. But land title systems are already being adapted to a computerised format. The prediction of the computerisation of land conveyancing was put forward in England in 1973 by Tapper.[89] Chief Justice Warren Berger made a similar suggestion in his address to the National Conference on Administration of Justice in the United States in 1976.[90] The process of computerisation has already begun in Australia. In Adelaide, for example, a system has been opened whereby, for a small charge, members of the public with an interest in land can make an enquiry and examine documents of a great variety of government recording systems, without the need of a trained intermediary. More than 30 terminals have already been established and more are planned. The implications of this technological development for the widespread distribution and reasonable prosperity of the legal profession needs to be watched. Although frequently, and properly, the subject of criticism for the faults of individual members and for collective faults, it is hard to dispute the importance of a highly trained, vigorous and independent legal profession for the successful defence of freedoms and of the rule of law. In this sense, the fate of the legal profession and the impact upon it of information technology is a matter which, at least in some Member countries, deserves attention.

INSTITUTIONAL RESPONSES

40. National and international: The variety and complexity of the issues raised in this paper, which are, in turn, some only of the legal aspects of informatics, deserves the attention of lawyers and administrators at a national but also at an international level. At a national level, the point is increasingly being made that the democratic legislature finds it difficult to cope with the complexity, sensitivity and pace of technological change, of which information technology is but a species of a broader genus.[91] The need for the allocation of adequate resources to allow a comprehensive and vigorous attack by home governments on the multitude of issues posed by informatics and TBDF is manifest. But it is rarely stated. In the United States, Mr. William Fishman spoke in terms that could probably be applied, with appropriate adjustments, to all Member countries:

Congress should increase the resources available to the Executive Branch to deal with the issues. I understand the need for budgetary austerity. But even a few million dollars would go a long way to permit the [United States Government] to match other countries' governmental resources in this area. Given the stakes, the current financial resources and the dozen or fewer people in the U.S.G. who work actively on this issue, must be substantially increased.[92]

41. At the international level, the Organisation can provide the kind of assistance it has offered in respect of privacy laws. OECD Guidelines can help to:

- harmonise rules as they are developed;
- inform Member countries of the standards being adopted elsewhere; and
- avoid the conflicts of laws that will all too readily otherwise spring up, through ignorance of, or indifference to the desirability of harmonious and compatible legislation.

The OECD is not the most appropriate international body to deal with all of the legal issues, domestic and international that have been mentioned. WIPO and the Hague Conference are clear candidates for the specialised problems of intellectual property and conflict laws. However, it is now increasingly realised that the law does not operate in a vacuum, that justice has a price and that a balance must be kept between the benefits and the costs of legal regulation. This realisation adds legitimacy to the increasing interest being shown by the OECD to legal concerns. It is not simply a matter of keeping an eye on the potential development of economically protectionist legislation which has been drawn ostensibly for the protection of privacy, intellectual property rights, business interests and so on. It is a matter of proper concern that, as technology, including information technology, presents common problems to the governments and people of like communities, experts and other representatives should come together to help in the design of harmonious and compatible laws, so far as these may be achievable. The alternative is the spectre of disharmonious and incompatible domestic laws, such as grew up to impede international trade in the 18th and 19th century. If they occur now, they will significantly diminish the advantages that will otherwise accrue to Member countries and their citizens from the remarkable information technology of our times.

42. Industry response: A proposal: For the International Information Industry Conference (IIIC) held in Quebec City, Canada, in June 1982 I listed some of the legal and social problems elaborated in this paper. Whilst acknowledging that the world information industry was not in the Santa Claus business (and indeed was not without problems of its

own), I expressed the hope of a greater realisation on the part of the industry of the responsibility it must share for the solution of the social and legal problems that attend its technological successes. I pointed out that ultimately the business of the industry was one of serving a peaceful, contented, law-abiding and safe community, including internationally. Social advance and acceptance must go hand in hand with technological change. The private sector in the international information industry should understand that it is in its self interest to help our societies to absorb and cope with the social and legal implications of the technology it is so successfully introducing throughout the world. The modesty of the present investment which such a prosperous, adventurous and fast developing industry makes for the study of the social, economic and political concerns of industry-wide dimension is such as fairly to attract criticism or even derision.

43. There is a natural and understandable tendency for the information industry to assert that the social and economic 'fall out' is a problem for government: for national bureaucracies or international agencies such as this Organisation. In some countries, such an attitude would be reinforced by actual resistence against industry involvement, because of the desire of home governments to distance themselves from what may be seen as foreign information industry giants. Sensitivity to this factor may have led to the private sector of the world information industry adopting a 'low social profile' - contributing to good works here and there, promoting good industrial relations with their staffs, supporting sporting contests widely publicised in the media, but otherwise keeping out of the concerns about social and legal change.

44. In my address for the IIIC meeting, I suggested that the multiplication of the problems of the new information order imposed obligations, if only in self defence, upon the industry. It is presenting the problems, many of them common, to governments and societies around the world but overwhelmingly within the Member countries of this Organisation, I proposed that an international centre for the study of the legal and social implications of informatics should be created, isolated from the industry sources of its funds, yet guaranteed of a flow of funds for a sufficient period of time to assure stability and to attract suitable appointments of the highest calibre. It should not be unrealistic to expect such a prosperous industry to provide funds for an Institute of Informatics and Society, to study the impact of the new information technology in those countries which are being penetrated most rapidly. The investment would be miniscule by comparison with the income and profits of the industry. It could be seen as a minor cost, a kind of insurance premium, to guarantee that those who present the problems play a more active part than they have in the past, in helping our societies to provide the solutions. We need lawyers and lawmakers who speak the language of the computerist, who understand the

ways they think and who can interpret the technology to a wider audience and facilitate the development of solutions that can be studied by national governments and international organisations such as this. It is my view that the number, complexity and pace of presentation of problems is now such as to require better support for the handful of national experts who are repeatedly burdened with the daunting and oppressive task of considering the implication of the technology throughout the OECD. The approach now being taken to the incidence of informatics is unworthy of an otherwise efficient industry. I repeat my view that, in addition to the institutional solutions being developed at a governmental level, both nationally and internationally, the private sector of the information industry should be doing more than it is to promote an orderly, systematic, well researched, interdisciplinary and independent consideration of the sociological, economic, moral and legal implications of informatics and TBDF. Legitimacy and acceptability would require independence. An institute captive of the industry, would command no respect. But the need to devote a tiny fraction of the profits being made, and properly made, from the remarkable advance of new information technology is beyond serious debate. Such an Institute could address, particularly the international problems, some only of which have been identified in this paper and others of which will emerge during this First Session.[93]

OF PROFITS AND PROPHETS

45. This review of legal issues has only touched the surface of the many questions that could be addressed. As we solve one legal problem or provide the ideas that will help to solve others, more present themselves and demand novel solutions. We are at an historic moment in the world legal order. A dynamic international technology is pressing forward the urgent need for the development of an effective, new international legal regime. From being the esoteric subject of a few specialists, international law as it affects the new information technology will increasingly become the concern of municipal lawyers, lawmakers and judges. It is important that the new legal regime should be developed in a coherent way and one which does not unduly impede the economies and efficiencies of the technology. This new Committee has a central role to play in these developments. It will need the gift of prophesy. I express the hope that the legal concerns which I have mentioned will not be lost in the headier and more familiar consideration of economic, social and technological concerns. What will it profit our societies if they advance remorselessly down the road of technology but lose respect for the law and their institutions and adherence to the rule of law?

ENDNOTES

1. World Future Society, 4th General Assembly, Communications and the Future, preliminary program, June 1982, 3.

2. See report by H.P. Gassmann, Draft Summary Record, OECD Working Party on Information, Computer and Communications Policy, 30, 31 March and 1 April 1982, (DSTI/ICCP/82.21, 5).

3. C. Tapper, Computers and the Law, 1973; C. Tapper, Computer Law, 1978; P. Seipel, Computing Law, 1977.

4. Esp. J. Bing, P. Forsberg and E. Nygaard, 'Legal Issues Related to Transborder Data Flows', Consultative Document for the OECD Expert Group on Transborder Data Flows (DSTI/ICCP/81.9), 1981. (Hereafter 'Bing').

5. P. Robinson, 'Legal Questions and Transborder Data Flow', paper for the Swedish and Norwegian Societies for Computers and Law, January 1982, mimeo, 1. (Hereafter 'Robinson').

6. ibid.

7. United Nations Centre on Transnational Corporations, 'Transnational Corporations Dominate Transborder Data Flows' in Intermedia, May 1982, Vol. 10 No. 3, 48, 55.

8. DSTI/ICCP/82.21, annex II.

9. As reported New Scientist, 3 September 1981, 606.

10. Australian Law Reform Commission, Discussion Paper No. 14 Privacy and Personal Information, 1980.

11. OECD, U.S. Delegation, 'The Legal Issues in Transborder Data Flow', June 1980.

12. For the decisions see DSTI/ICCP/82.1, 7.

13. Robinson, 2.

14. Bing, 5-6.

15. OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1981, Explanatory Memorandum, 13, 15 ff.

16. ibid, 18-19.

17. Bill C-43. An Act to enact the Access to Information Act and the Privacy Act, to amend the Federal Court Act and the Canada Evidence Act, and to amend certain other Acts in consequence thereof.

18. ibid, s 12(1).

19. New Scientist, 3 September 1981, 605. Note that the OECD has decided to examine compliance with the Guidelines annually. DSTI/ICCP/82.21, 15.

20. O.H. Ganley and G. D. Ganley, To Inform or to Control? The New Communications Networks, 1982, 85-86.

21. New Society, 26 March 1981, 547.

22. Economist, 25 October 1980, 81.

23. United Kingdom, 'Data Protection. The Government's Proposals for Legislation', 1982. For criticisms see (1982) 132 New Law Journal 357.

24. 'When Privacy Laws Hurt Trade', Business Week, 14 April 1980, 104 G.

25. Austria, Denmark, Luxembourg and, in part, Norway. See M. E. Hogrebe, 'Legal Persons in European Data Protection Legislation: Past Experiences, Present Trends and Future Issues', OECD Consultative Paper, DSTI/ICCP/81.25.

26. New Scientist, 3 September 1981, 604.

27. Hogrebe, n 25 above.

28. Cf annex III (Program: Australian Proposals), DSTI/ICCP/82.21.

29. Bing, 68.

30. OECD, ICCP Newsletter No. 6, June 1982, 8.

31 A. Siegel, Communications and Politics: Canada's Cautious Steps Toward Open Government in (1980) 7 Canadian Journal of Communication, 20, 21.

32. ibid, 22, 27.

33. For example, the so-called Watergate affair. Siegel, 27.

34. ibid, 30.

35. Transnational Data Report, Vol V No. 1, 36 (Jan-Feb 1982).

36. T. Riley, 'Just Access' (1980) 10 Australian Social Welfare Impact, 8.

37. See e.g. Administrative Decisions (Judicial Review) Act 1977 (Aust.), s 13.

38. Bing, 15. Cf. Freedom of Information Act 1982 (Aust) s 4 defines 'document' to include (amongst other things) 'any article or thing that has been so treated in relation to any sounds or visual images that those sounds or visual images are capable, with or without the aid of some other device, of being reporudced from the article or thing...'. Section 17 specifically provides for requests which involve access to computerised information. It requires the agency to deal with the request 'as if it were a request for a written document so produced [by the use of a computer or other equipment].

39. Bing, 32.

40. Bing, 57.

41. D.C. Rowat, 'Scandals Add to Pressure for Public Access Law' in Transnational Data Report Vol V No. 1, 37 (Jan-Feb 1982).

42. Robinson, 3-4.

43. Report by Swedish Government Committee (SARK), The Vulnerability of the Computerised Society: Considerations and Proposals, 1979 (official English translation by J. Hogg), 1979.

44. The terms of reference are contained in OECD, ICCP Newsletter, No. 5.

45. DSTI/ICCP/82.21, 9.

46. Canadian representatives expressed concern that by 1985 100,000 jobs would be lost from Canada to the United States. New Scientist, 3 September 1982, 605.

47. Ward v. The Superior Court of California 3 CLSR 206 (Cal) (1972).

48. U.S. District Court for the District of Maryland, Crim. No. 76-079H, cited Bing, 14. Cf. Hancock v Decker 379 F. 2nd 552 (1967) discussed in J. Bing 'Information Law?' in (1981) 2 Journal of Media Law and Practice 219.

49. Robinson, 4.

50. [1975] 2 All E.R. 146. Discussed, J. Crawford, 'Decisions of British courts during 1974-5 involving questions of public and private international law', The British Year Book of International Law, 1974-1975, 341 at 361f.

51. Cf The House of Lords (England) in Treacy v. Director of Public Prosecutions [1971] AC 537.

52. Director of Public Prosecutions v. Stonehouse [1978] AC 55; [1977] 2 All E.R. 909. Discussed J. Crawford. 'Decisions of British Courts during 1978 involving questions of public and private international law' in The British Year Book of International Law, 1978, 259 at 279.

53. Ward v. The Queen (1980) 29 Australian Law Reports 175. See also M.D. Kirby, 'The Computer, the Individual and the Law' (1981) 55 Australian Law Journal 443, 454. Cf S. H. Nycum, 'The Criminal Law Aspects of Computer Abuse' 5 Rutgers Journal of Computers and the Law 297 (1976).

54. OECD Guidelines, Explanatory Memorandum, n 15 above, 36.

55. ibid

56. OECD Guidelines, para 22.

57. Testimony of W. L. Fishman, United States Banking Committee Sub-Committee on International Finance and Monetary Policy, 9 November 1981, mimeo, 10-11. (Hereafter 'Fishman').

58. United States Delegation, n 11 above, 4-5.

59. See also V. A. Assevero, 'Liability for Errors in Electronic Transborder Data Flows', OECD Consultative Paper, DSTI/ICCP/82.23 where practical illustrations are given.

60. Bing, 65.

61. ibid, 65, 68.

62. Resolution of the OECD Council, adopted at the 557th Meeting 1 April 1982, para 3.

63. Fishman, 2-3.

64. ibid, 4.

65. J. de O Brizida, Address at the Opening Session of the IBI World Conference on Transborder Data Flow Policies, reprinted Transnational Data Report, July/August 1982, 33.

66. New Scientist, 3 September 1981, 604.

67. A.A. Bushkin, 'A Status Report on the Evolving U.S. Positions on Trade and International Communications', mimeo, Telemation Associates Inc, 12 February, 1982, 3.

68. Robinson, 3. The notion of sovereignty can extend to extra-territorial legal effects to the extent of matters having some connexion with the territory of the country concerned.

69. Bing, 28-37.

70. Bing, 11.

71. Niblett cited Bing, 12.

72. Bing, 81.

73. Bing, 56. Cf. 'Coditel' decision of the European Court of Justice there referred to, reported Transnational Data Report, Vol IV No 1, 1981 (January 1981), 7.

74. Robinson, 3.

75. A.N.Yiannopoulos, The Unification of Private Maritime Law by International Convention, 30 Law and Contemporary Problems 370, (1965).

76. Fishman, 5-6.

77. ibid, 6.

78. OECD, ICCP Newsletter No. 6, 5.

79. Bing, 19, 53.

80. Assevero, 18.

81. Punch, 13 February 1963.

82. These are discussed by Bing, 8-12. See cases there cited.

83. Assevero, 16.

84. R. David and J. E. C. Brierley, 'Major Legal Systems in the World Today', (2nd ed), 1978, 328.

85. Civil Evidence Act 1968 (Eng), s 5. As to the United States position see 'A Reconsideration of the Admissibility of Computer-Generated Evidence' in 126 Uni of Penn L Rev 425, 438 (1977).

86. The Australian statutes are collected in Kirby, n 53 above, 452ff.

87. Guardian Gazette, Vol 79 No 14, 21 April 1982, 1. ('Speedsend' transmission service announced).

88. Bing, 81.

89. C. Tapper, 'Computers and the Law', 299.

90. 44 U.S. Law Week, 2488 (1966).

91. B. Jones, 'Sleepers, Wake!', Technology and the Future of Work, Melbourne, 1982.

92. Fishman, 7.

93. Cf R. Levesque, Discours a l'Occasion du Congres International de l'Industrie Informatique, mimeo, 1 June 1982, 7.