

74.1

ASIA PACIFIC FOUNDATION OF CANADA

ATWATER INSTITUTE

PACIFIC CO-OPERATION AND INFORMATION TECHNOLOGY

PACIT 88

"INFORMATICS, TRANSBORDER DATA FLOWS & LAW"

INFORMATICS, TRANSBORDER DATA FLOWS & LAW

Hon Justice Michael Kirby CMG

SUMMARY

This paper begins by illustrating the enormous opportunities presented to Pacific rim countries by the development of informatics and transborder data flows (TBDF). But from the legal point of view, there is a problem. It is essentially that law is local whereas the technology is pervasive and universal. Unless this basic dilemma is solved, the risk is run that local laws will operate on TBDF in inefficient and unpredictable ways. Or that laws of the information-powerful countries will stamp their values and cultures upon the information-poorer. The basic theme of the paper is the need for new international meeting points and institutions to develop new basic principles of law which are as radically different from past approaches to legal regulation as the new technology is different from the past media of communicating information.

One example of a generally successful international effort to draw up guidelines on the impact of TBDF were the OECD Guidelines on Privacy, adopted in 1980. But the author's thesis is that these Guidelines themselves need updating and only deal with one of the many topics requiring attention. The need for updating is shown by the experience in the operation of early privacy laws and by recognition of the privacy

intrusive capacity of free text and other new technology which render earlier principles inapplicable or insufficient.

The other legal areas requiring attention include:

- \* The interactive operation of Freedom of Information Laws;
- \* The interactive dependence upon flows from other jurisdictions, which heightens vulnerability and the impact of data crime;
- \* The rules on conflicts of laws to choose the applicable law where several jurisdictions are involved in TBDF; and
- \* The development of new principles for intellectual property law, adapted to the new media of informatics.

The paper closes with an appeal for closer cooperation between Pacific rim countries in work on the legal and social implications of TBDF. In microcosm, the Pacific presents the world's problem of adapting local law to universal technology.

ASIA PACIFIC FOUNDATION OF CANADA  
ATWATER INSTITUTE  
PACIFIC CO-OPERATION AND INFORMATION TECHNOLOGY  
PACIT 88

INFORMATICS, TRANSBORDER DATA FLOWS AND LAW -  
NEW CHALLENGES

The Hon Justice Michael Kirby CMG<sup>\*</sup>  
Australia

CENTURY OF THE PACIFIC

The Economist newspaper recently declared that the twenty-first century will be the century of the Pacific. Countries which border the Pacific, therefore may have reason to celebrate their good fortune. They should prepare to make the most of it.

The twentieth century has seen tremendous changes in the Pacific, as elsewhere in the world. The century dawned upon a Pacific Ocean dominated by European colonial powers. It was only in 1905, with the Russo-Japanese War, that the signal was sent out that a new era was dawning. Two World Wars later and after terrible conflicts in Korea and Vietnam, the situation at the end of century is becoming more clear. Countries such as Canada, Australia and New Zealand which began the century as European outposts of the British Empire close it as independent nations. They have their own identities and a growing realization that they must make their mark - economically and culturally - in their environment, including the Pacific. Other countries have thrown off the colonial yoke. The colonists have sailed away, only sometimes to be replaced by other colonists closer to home. The indigenous movement is

strong, as has lately been demonstrated by events in Fiji, West Irian and New Caledonia. Latin America remains a sleeping giant of great resources still barely integrated into the community of the Pacific. Two great powers have emerged with their own separate claims profoundly to affect the future of all Pacific nations. I refer to Japan and China. New nations of enormous and previously unsuspected economic importance have emerged to an influence which would seemed impossible even a decade or so ago. I refer to Singapore, Taiwan (China) and the Republic of Korea. The position of Hong Kong, as 1997 approaches, presents fascinating questions. And, over all, the brooding presence of the two super powers - the United States of America and the Union of Soviet Socialist Republics face each other across the Pacific Ocean.

On my way to conduct a mission for the International Commission of Jurists in Palau in Micronesia in January 1988, I gained some insight into the vastness of the Pacific Ocean. Touching down at the little islands scattered across this blue emptiness, I realized the significance of the expression "Pacific rim". It is the nations that circle the ocean that lay a claim to the twenty-first century. Between them, atolls and a few islands apart, there is no impediment but distance and ocean. Across that ocean run the cables that link the information systems of the bordering states. Soon the COMPAC cables will be supplemented by optic fibres which will increase greatly the quality of transmission and expand enormously the quantity. Over the Pacific come the wireless messages. Higher

still are the satellites promoting the global village. Vast amounts of trade already pass across the Pacific. Vast too is the data flow between the Pacific rim countries. In a sense, these countries are a microcosm of the rest of the world. The issues raised for them by transborder data flows (TBDF) are similar to the issues raised for countries everywhere. But within Europe there are established institutions, including the Council of Europe and, by now, settled media for developing policies and even laws on the social problems thrown up by TBDF. So it is between the powerful economic forces of North America, between the common law countries of Oceania and the countries of Latin America with their strong linguistic and cultural connections.

The problem presented to the lawyer by TBDF between the Pacific rim countries can be stated in a sentence. It is that the technology of informatics is universal, pervasive and common, whilst the legal systems of the Pacific rim countries are as diverse as it would be possible to imagine. Whereas Canada, the United States, Australia, New Zealand, Hong Kong and a few island countries share the common law derived from England, the countries of South and Central America follow the civil law tradition. With adaptations, so do the Soviet Union and those Asian countries formerly colonised by France. Japan adopted aspects of the civil law system, following the Meiji reforms. But onto that system has been grafted, since the Second World War, aspects of the common law system of judge-made law. China, keen to take advantage of economic development and international trade, is in the process of a

remarkable re-establishment of legal institutions and respect for the Rule of Law. All of this is to oversimplify the differences. But enough has been said to point to the deep-seated variations which exist between the legal systems of the countries surrounding the Pacific.

In a conference of information technologists, there is the common language of the technology. In a conference of medical practitioners, there is the common object of the human body. But in a truly international conference of lawyers, there is great difficulty in finding common concepts and a common object. The problem is not simply one of language, although that is hard enough. Nor is it simply one of different institutions which frame the approach to the perception and the categorization of legal issues. The overwhelming problem is that law derives from jurisdiction. Jurisdiction is local. In nations like Canada, the United States and Australia, there is not even a single system of law. Federal systems divide power and, thus, law. Accordingly, to the multitude of legal systems of the nations surrounding the Pacific must be added the sub-systems within each Federal country.

The result is that the Pacific rim, linked so intimately by unbroken ocean, is divided by legal systems of great diversity. The countries of the Pacific rim, joined by cable, wireless and transborder data flows are divided by a cacophony of laws which inevitably impinge upon the pervasive, universal, common technology of informatics.

The common links force upon those that are linked, a

degree of co-operation and rationalization of the differences of their legal regimes. So powerful is the force of information technology, and so decentralised its use, that attempts to enforce upon it idiosyncratic local laws would frequently fail. More importantly, the links necessitate co-operation. This has resulted in steps being taken to promote knowledge of the differences of law, particularly in areas such as business law. In this regard, Canada has taken important initiatives. A Speakers' Bureau on Asian Business Law has been established. The first Annual conference of Asian Business Law was held in Montréal in August 1988 in conjunction with the Canadian Bar Association Annual Meeting<sup>1</sup>. Steps are being taken to promote contact between lawyers in different countries of the Pacific rim. Detailed analyses are beginning to appear in law journals concerning the basic concepts of the legal systems of other Pacific rim countries<sup>2</sup>. These are desirable initiatives. But they remain very much in the minor key. They appear unlikely to be an adequate response to the multitude of legal issues which present for urgent resolution, as a result of the impact of informatics on the diverse legal systems of the Pacific.

It is in this connection that more radical proposals appeal to the imagination. Thus, former Japanese Prime Minister Yasuhiro Nakasone captured a great deal of attention when, in April 1988, he proposed the creation of a "Pacific version of the OECD". He was speaking at the Trilateral Commission in Tokyo<sup>3</sup>. He called for the setting up of a "loose organisation" in which exchanges of capital, technology,



goods, information, academic research and culture could be promoted in an "efficient and co-ordinated manner" amongst the nations concerned. He suggested that there was a need for more active co-operation in the Pacific region. And he put his proposal in the context of the remarkable developments which are occurring, both in the Soviet Union and in China towards greater openness of administration and of trade. It is not purely coincidental that these developments have coincided with the advance in information technology. It is a truism that information is power. It is also a modern truism that information technology is the key to economic progress. Accordingly, the coincidence of the world-wide moves to liberalize the legal regimes governing information technology and trade generally, with the move toward greater openness in the political and trading policies of the Soviet Union, China and other formerly closed societies, can be seen as aspects of the one movement. It is a movement at once international in its dimension, technological in its stimulus and optimistic in its political implications. The question for the thoughtful lawyer is how might he or she act so as to diminish the impediments which the provincial discipline of the law provides to these great movements of trade, technology, politics and culture.

I have now put the dilemma of my paper sufficiently in context. It is a simple dilemma, easy to describe. Universal, pervasive technology. Local, diverse law. The interaction of these apparently incompatible forces provides a challenge not only to the intellect but also to business necessity, political

progress and institutional arrangements. The business necessity was well described in an explanation by the Vice-President of the American Express Company of the importance of TBDF to her organization. She said:

"American Express, like other multinational corporations and especially service sector corporations, relies on automated, reliable and cost-effective global communication networks for the majority of its international operations. We have data processing centers around the world - including Brighton, Hong Kong, Singapore and Bahrain - all of which process data from, and disseminate data to, many different countries. Our card business depends on global communications networks. There are over 1 million non-dollar American Express cards in force in twelve currencies. The majority of these accounts are processed through our European processing center - approximately 2.5 million transactions per month. The central European data base for card members is located in England and accessed throughout Europe. The central authorization system for our card relies on a data base in the United States. If open access were impaired American Express would encounter difficulties in providing a full service to its card members and be forced to decentralize at considerable cost. Communications are also essential for other internal operations; personnel records, in-house communication lines, internal budgetary procedures - all depend on our ability to transmit and store information within and across international boundaries. Finally, but very significantly as a result of these operations, American Express holds a vast amount of confidential information on our customers".<sup>4</sup>

The importance of TBDF in economic terms can scarcely be overstated. Obvious benefits derive from continuous and uninterrupted flows of information between nations. Economic value attaches to information. Accordingly, there is a need to protect trade in it by generally accepted standards of fair competition. On the other hand, law exists to defend human rights, the concerns of business and other organizations and

national interests deemed appropriate for protection by the local legislature, courts and administrators. For this reason, it is understandable that local law should lay down standards which are considered appropriate for the protection of such values as privacy, business secrecy, intellectual inventiveness and so on. In a nutshell, the basic problem that is presented by TBDF is one of:

- [a] reducing the impact of ineffective and inefficient laws which impinge upon the flows of data that are generally beneficial to humanity;
- [b] whilst at the same time assuring the effectiveness of those laws which are considered necessary to uphold basic standards, deemed appropriate and desirable by local legislators, legislators in several jurisdictions or even international agencies collecting together the representatives of many states.

The alternative to a rational approach to the legal problems presented by TBDF is obvious. Either we surrender ourselves to wherever the technology takes us, doing so wholeheartedly in the belief that it will lead, anyway, in the right direction or reluctantly, because we feel incapable of doing otherwise. Or we surrender the regulation of the technology to the laws of the most potent states with the most economic muscle operating on the technology. To do this may be to surrender cultural values important in the local jurisdiction and submit to the legal standards which are deemed appropriate in another jurisdiction, eg the United States or Japan. A third possibility is that a cacophony of laws will impinge on TBDF in a haphazard, unpredictable and unexpected

way. The result of this would be legal chaos, with an inefficient interruption to free flows of data or gross uncertainty about the legal position of such flows. Such inefficiency and uncertainty would impose an opportunity cost because of the inhibitions upon trade and development which can arise in that situation.

All of this should suggest the obvious conclusion. This is that, with an international technology as pervasive as informatics and as global as TBDF, international agencies should be established to provide meeting points for the resolution of problems in a way that is at once compatible with maximizing the greatest possible free-flow of data and at the same time optimizing the protection of values which are shared and maximizing other values which are held generally in common.

For more than a decade, now, observers of the TBDF scene have been urging the need for appropriate institutional solutions to the social, cultural and legal problems presented by this phenomenon. Opinions about the nature of the institution necessary to provide the leadership required on these topics differ, as do the perceptions of the urgency of providing solutions. On a global scale, the contribution of the United Nations Organization and its agencies, including UNESCO, has been disappointing in this regard. So too has the contribution of the Intergovernmental Bureau for Informatics in Rome. Specialized agencies have done their own thing. The one global organization which has provided important leadership is the Organization for Economic Co-operation and Development (OECD). That body has done vital work in the field of

privacy<sup>s</sup> and also in the areas of intellectual property and information crime. But in recent years there has been a distinct lack of momentum on these issues in the OECD as it has addressed itself principally to technological and trade aspects of TBDF. The social and legal implications have definitely been relegated to a comparatively lesser concern. The essential question that is presented by this paper is whether that relegation is justified. Or whether, as it is suggested, the range, complexity and urgency of the issues presented to our societies and their laws by TBDF necessitate that with a heightened sense of urgency, institutional means should be obtained to provide, some of the solutions. The balance of this paper will be devoted to identifying some only of the legal questions which are raised by TBDF. If the OECD is not willing or able to provide the same impetus which led to the OECD Guidelines on Transborder Data Barriers and the Protection of Privacy in 1980, in the other legal fields requiring attention, it is possible that the Pacific rim countries should look elsewhere. Around the Pacific rim is a family of nations that extends far beyond the twenty-four member countries of the OECD. It is true that they do not have the same commonality of political and economic systems which provides the large potential, within the OECD, for effective co-operation. On the other hand, the political and economic differences have diminished somewhat of late. And the commonality of the technology behind TBDF certainly presents an incentive to exploring common solutions to the social and cultural questions that are raised. In default of OECD or wider global

initiatives, it is possible that Mr. Nakasone's suggestion should be taken further so that some of the social and legal questions raised by TBDF could be studied on a Pacific-wide basis.

#### LEGAL ISSUES

##### Privacy Protection:

The period between 1973 and 1980 saw enactment of a large number of laws on privacy (data) protection. Many of these were stimulated by perceived problems in information technology. A concern was then expressed in many circles that these laws, if they shared no common principles and accepted different machinery for enforcement, might actually impede TBDF and have an undesirable economic impact on the flow of data and of trade. The result of this concern was, amongst other things, the establishment of the OECD Expert Group which developed the Guidelines on the protection of privacy and transborder flows of personal data. The Guidelines were recommended in 1980 to the Council of the OECD. They were adopted by it. Since then, all member countries of the OECD have adopted the Guidelines. Many of them have either adapted pre-existing privacy (data) protection laws or have enacted new laws to secure harmony with the OECD principles. In other countries, although laws have not yet been enacted, recommendations have been made for the enactment of laws drawing on the OECD principles and court decisions have begun to draw upon them for development of common law. It is in this way that it seems likely in the future that, with common technology, principles will be developed in international

agencies which can then be adopted by countries affected by the technology so as to ensure a general harmony in the approach of the law. So much is simply a recognition of the difficulty and inefficiency produced by idiosyncratic regulation of common technology. The same lesson exists in relation to developments of biotechnology as of informatics.

In addition to the legislation just referred to, sectoral standards have been adopted, as for example in the Council of Europe. Furthermore voluntary compliance with the OECD Guidelines has been adopted in a number of places as a suggested alternative to legislation. Thus, in the United States, a large number of companies have accepted the OECD Guidelines for corporate self regulation. In Canada, the Secretary of State for External Affairs wrote in December 1986 to approximately one hundred and fifty chief executives recommending implementation of the OECD Guidelines as corporate policy. The Canadian Bankers' Association model privacy code is obviously derived from the OECD principles. In Japan, the government also encouraged the use of the Guidelines as a model. It led, in February 1988, to the publication of voluntary guidelines for the protection of personal data in financial institutions. These, and other developments of privacy protection are well described in a paper prepared by Mr G Tucker for the OECD Secretariat.<sup>6</sup>

Many of the OECD member countries with data protection laws include some provisions for regulating international transfer of personal data. However, the nature of these provisions varies widely. It seems generally accepted that the

adoption by the United Kingdom of its Data Protection Act 1984 was less the result of an acceptance by the Thatcher government of the need for this additional form of regulation of a fast developing technology, still less a tender concern for the human rights issues involved, so much as an appreciation that, without such a law, United Kingdom data processing would not be able to participate freely in the European market<sup>7</sup>. The United Kingdom Government's delay in preparing legislation had already led to the loss of contracts for data processing from some European countries whose laws required legal protection if personal data on subjects within their jurisdictions were to be transferred to another country (as the United Kingdom) which did not, by law, guarantee such protection. This is one way by which international enforcement of data standards is secured, even in the pervasive world of transborder flows of personal data.

In some countries, TBDF are treated by legislation as just another aspect of the transfer of personal data so that no special requirement exists in relation to it. This is the approach taken in the Federal Republic of Germany. In Austria, on the other hand, in some circumstances the data user or collector must be granted a licence before any personal data is transmitted, although the circumstances in which the licence must be sought have recently been reduced in number. The law in France, Finland and Norway permits the free flow of international personal data, subject to an overriding discretionary power of the relevant authority to prohibit or regulate such activity. Advance notice of intended data flow



of this kind is required to the central authority prior to the transfer occurring. By way of contrast, in Sweden and Iceland, the prior permission of the data protection authority is generally required before any international transfer of personal data is lawful, where such data would fall within the provisions of the legislation. Mr Tucker comments that common law countries such as Australia, Canada, New Zealand and the United States, which do not have provision akin to that enacted in the United Kingdom, may already be suffering adverse consequences when entering into trade in data services where the country in which the other trader resides has data protection laws which prohibit the transfer of personal data to countries without equivalent protections.<sup>a</sup>

A new issue now under consideration in this connexion is the so-called "second generation" of data protection legislation. This expression has been taken to apply to a new law in Finland and the proposed law in the Netherlands. Such laws favour notification and registration rather than the bureaucratic and cost intensive authorization or licensing systems. They tend to cover manual as well as automated systems. They tend to include specific sectoral rules to take account of particular problems of particular data users. They reserve a place for self-regulation and they limit the enforcement role of the data commission, reserving such functions to administrative bodies or the courts.

It is inevitable that more attention should be given to the success or otherwise of the operation of the OECD Guidelines, ten years after they were adopted. No more in

international than in national laws should it be assumed that the mere passage of the rules will secure the desired effect. There is a constant need to update rules such as the OECD guidelines. Nowhere is this more necessary than in the interaction of rules with a technology which is constantly and radically changing.

Data processing has changed in the last decade from file orientation to data orientation. The significance of this change has been recognized in the Council of Europe:

"The solutions envisaged in the 1970s were valid insofar as they were brought to bear on the then state of the art, characterized by main frame - stand alone computers with dedicated applications capable of storing and processing data on "identified or identifiable individuals" on a "file" under the authority of a "file controller" identifiable at will by a "supervisory authority"9.

In evaluating the appropriateness of the OECD Guidelines, a decade later, it is necessary to challenge some of the "tacit assumptions" about the technology, as those assumptions apply to the current technology. Free text systems allow searchers to create specific information which is not ordinarily accessible to the data subject nor even sufficiently capable of control by a "purpose limitation" requirement. Data bases today are frequently built on the assumption that they will be used without regard to the purposes for which they were set up and even the purposes for which the data has been stored. In this way, modern systems may not be apt for the application of the existing principle of transparency. Personal identifiers might not, as such, be

used in the collection of the data. But modern search techniques may permit "hidden" information to be derived from raw sets of personal data.

These and other changes in the technology require a constant reconsideration of the principles adopted by the Council of the OECD. This in turn presents one of the additional sub-dilemmas of regulation of TBDF, both national and international. The languid, time-consuming, laborious task of deriving principles on TBDF by meetings of international experts may simply not be adequate for the range or variety of the problems presented by modern information technology and especially its international face : TBDF. Obviously what is needed is a constant interaction between rule makers and technologists. Institutions of rule making need to have as many technologists as they have lawyers. Lawyers are needed who are informatics literate. Technologists are needed who are alert to the moral, social and legal fallout of the technology as it operates.

There are many additional problems which were not addressed in the OECD Guidelines. They now have greater urgency because of the passage of years in which little has been done to address them. Thus, attention should be paid to the extent to which legal, as distinct from natural, persons have the kinds of rights which are expressed in the OECD principles. Are those principles, at base, human rights apt for the technological age? Or are they aspects of the efficient flow of data and thus equally applicable to legal

persons (corporations, firms, associations etc)? A code of ethics is needed in the informatics industry to permit fine tuning of matters of detail in the fair handling of information, particularly personal information. The implications of privatization of telecommunications agencies, which carry so much personal data, need to be considered. The development of privatization is today so well advanced in several countries that experience should now be available as to whether the loss of the PTT monopoly has caused personal data to haemorrhage. It would be surprising if there were not more reports if this had occurred.

Freedom of information:

A further consideration relevant to TBDF is the development of freedom of information legislation (FOI) in many countries. Such laws now exist in Canada, the United States, Australia, New Zealand and several other countries of the Pacific rim. In a sense such laws must be seen as the administrative catchup to the political developments of representative democracy attained in many countries in the nineteenth century. The object of FOI is to remove bureaucratic "rotten boroughs" and to provide for the true accountability of those in the public sector who make important decisions affecting individuals.

The passage of FOI legislation, in different terms, with different exemptions and different machinery of evaluation, can give rise to legal problems as a result of TBDF. Professor Jon Bing of Oslo has reported on the conviction for a security offence of a Norwegian social

researcher who published certain findings on NATO defence arrangements which were contained in documents access to which was restricted under Norwegian law. The documents had been retrieved in Norway on line, pursuant to the United States Freedom of Information Act<sup>10</sup>. Similar examples abound in many countries around the Pacific. In Australia, documents on defence matters which are not accessible in Australia and would not be accessible under Australia's FOI law, have been secured without impediment from the United States under its FOI law. In Japan, a civil action was brought against makers and distributors of an antibiotic alleged to have caused a rare blood disease in the plaintiff. Before 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 then obtained the self same information from the Food and Drug Administration of the United States under a request filed in that country pursuant to its FOI Act<sup>11</sup>.

The new element in this equation is provided by the new technology. What might be inaccessible, even strictly secret, in one country might be readily accessed elsewhere, or even in the same country because of the technology of TBDF. The lesson of this development is that new information technology is likely to hasten the influence of openness of administration under FOI law for the simple reason that once information has haemorrhaged, it is difficult to re-contain it. The United Kingdom Government discovered that simple

fact in its world-wide endeavours to prevent the publication of the book by Mr Peter Wright Spycatcher, revealing secrets derived during his time working for MI5.

Vulnerability and crime:

The issues of vulnerability caused by TBDF were first gathered together in the Swedish government's report of 1981 on the Vulnerability of the Computerized Society<sup>12</sup>. Since then, there has been a growing appreciation of the dangers which are presented by the interdependence that flows from TBDF. For example, during the illegal detention of hostages in Iran, a number of United States journals suggested limitation on Iranian access to data processed in the United States. In the past, assets of enemies were frozen. How much more leverage would be secured, in modern circumstances, by the freezing of access to data vital to the domestic economy of an adversary?

This issue is not entirely theoretical. Perhaps more than any other country, Brazil has designed a full set of policies to deal with TBDF. Its efforts arose out of a national computer policy which aimed to create a national computer capability. Since 1972, a federal agency in Brazil has supervised the use and acquisition of computers. In 1978, legislation required that all transnational computer communication systems should be subject to the approval of the agency. 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 Brazil<sup>13</sup>. The fear of the

spread of such legislation both in Brazil and elsewhere led to the coining of the catch-phrase of a "world data war". It was one of the stimuli to the initiatives, including in the OECD, to break down the disparity of legal rules and to promote TBDF by the commonality of those rules and by the adoption by a principle of general free flow of data. That principle was in turn reinforced in April 1985 by the adoption of the OECD of the Declaration on Transborder Data Flows. With due regard to national laws, this declaration enshrined the intention of member countries to promote access to data and information related services and to avoid the creation of unjustified barriers to TBDF.

More complicated is the question of informatics crime. This is, in a sense, one aspect of the greater vulnerability of the "wired society". Such a society, including the international interconnected community, is more susceptible to damaging antisocial conduct because of computer terrorism and computer crime. There is an acute need to adjust the definition of crime and to develop agencies for dealing with it when confronted with the problem of crime in TBDF. This need arises from the fact that crime is typically strictly defined. Many of the old definitions simply do not fit the new problems. Thus "theft" at common law involved taking away the goods or articles of another whereas with data theft, it is the information which may be taken and not the hardware or software<sup>14</sup>.

The result of the realization of this fact has led to amendments of local criminal law in order to embrace

antisocial conduct which would otherwise slip outside the current definition of crimes<sup>15</sup>. A vivid, recent illustration of the problem was presented in a decision of the English House of Lords handed down on 21 April 1988. The case involved The Queen v Gold and Schifreen. By means of a dishonest trick, the defendants gained unauthorized access into and used a computer network by entering a number and password on a keyboard. This caused electronic impulses to affect a part of the computer known as the user segment. This cleared itself on the number and password being checked automatically by the computer. The overall time involved was momentary. The defendants were what is now known as "hackers". They were ultimately indicted on counts of forgery. At the close of the case for the prosecution, their lawyers submitted that there was no case to answer in law. This submission was rejected and the defendants were convicted. On appeal to the Court of Appeal, the appeal was allowed. The defendants were discharged. The prosecutor appealed to the House of Lords. But the Lords dismissed the appeal. They held that the process whereby the number and password were held momentarily in the control area of a computer for verification before being irretrievably expunged was not a process to which the words "recorded or stored" in the legislation under which the defendants were charged, applied. The Lords held that those words connoted the preservation of information for an appreciable time with the object of subsequent retrieval. Accordingly, they held that the defendants had not breached the strict terms of the Act.



They fell outside its prohibitions. In this way the hackers were able to escape liability under English law. The case illustrates the traditional precision with which criminal law is framed and interpreted (because it concerns the liberty and reputation of the citizen). It also shows that, even when an attempt has been made to enact legislation to catch computer crime, the attempt may fail on technical grounds - partly because of an inadequate understanding by the drafters of the technology or simply because the technology has overtaken the draft which was formerly adequate<sup>16</sup>.

A committee of the OECD has for some time been looking at aspects of computer crime. The potential of computer-related crime is now well recognised particularly in the fields of stealing data, illegally transferring funds, forging data, infringing security measures, etc. - all of which can be truly transnational. Other international bodies are also looking at aspects of computer crime as it concerns TBDF. For example, the Council of Europe is preparing to issue specific guidelines on the subject to influence the law-making of member countries. Obviously, international safeguards will be more effective if security measures are based on clearly defined and internationally accepted principles. But even this will be inadequate unless there are well established procedures and criteria for measuring the security of computer systems, detecting invasions and misuse, investigating offenders and ultimately bringing them to book in courts which have jurisdiction to deal with them.

### Conflicts of laws:

The sudden development of the new information technology has also presented difficult questions concerning the application of domestic laws. These questions transcend the particular problem of information crime. If an electronic message is generated in country A, switched in countries B and C, transits countries E, F, G and H, is processed in I and J, stored in country K and involves entities residing in and operating in other countries, whose law applies to it? What law applies to data processing carried out by a computer on an orbiting satellite? These are some of the problems which were called to attention nearly a decade ago by Mr William L Fishman<sup>17</sup>. His call coincided with the appeal in the OECD Guidelines on TBDF that 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". Since that well-meaning but somewhat ineffectual plea was voiced, nothing much has happened to clarify the statement of applicable private international law principles as they concern TBDF. The Hague Conference on Private International Law specializes in studying conflict of law problems. It has twenty-nine member countries including the United States, Canada, Japan and Australia. But Hague conventions typically apply to international sales of goods. So far, they have not been concerned with ephemeral electronic signals provided by informatics.

To some extent the solution to the problem of private

international law presents itself in different jurisdictions by the terms of the local legislation. To some extent, the problem is solved by the closed "club" of users of some of the most important TBDF systems. Thus, for example, the international SWIFT interbank transaction network has developed its own special conditions governing its network. It has hardware and software tailored for a club. But as TBDF increases and diversifies beyond the narrow confines of such a "club", complex questions of applicable law and also of liability arise which demand answers. At the moment, the technology here is developing in a "regulatory vacuum".

Intellectual property law:

Traditionally, intellectual property law developed around protections which were attached to the medium rather than the content of valuable information. It was not possible to patent or copyright an abstract idea. Patents attached to "inventions". Copyright attached to an original "work". The law of confidence and the law of defamation attached their consequences typically to the act of unwarranted communication or publication rather than to the information itself. The problem posed by information technology is that data (and therefore information) have now become liberated from the physical objects representing the data. Thus it has become possible, technologically, to read the text of a book without purchasing the book or even copying the text. Information technology has, in this way, made information, as such, a valuable commodity.

Because intellectual property law has traditionally

attached itself to physical objects, the information has, in the past, been regulated only indirectly. The question now posed is whether this is still an apt means for achieving an appropriate social balance between inventors and users of information based systems, in the age of TBDF. The added difficulty is provided by the fact that information produced in one country may be reproduced in ephemeral form in another. Therefore, unless arrangements can be made, recompense to the original author may be entirely avoided.

A recognition of this problem led to the establishment of committees in UNESCO and in the World Intellectual Property Organization (WIPO). The OECD has also taken initiatives to examine, in quite a novel way the issues of intellectual property law presented by informatics and TBDF. In a recent paper for a high level meeting of the OECD Committee for Information, Computer and Communications Policy, the Secretariat raised commendably radical questions about the possible failure of legal minds to catch up with the enormous potential of informatics and TBDF for the massive flow of data that comes in the train of the new technology. Until now, domestic regulators have moved with a degree of speed to plug the holes in the dykes presented when current copyright laws are held not to cover software<sup>1a</sup>. But should this be so? Should there be a more radical approach to the law on intellectual property right protection because of the radical difference between the old media and the new technology of informatics?

The OECD paper raised the question of how far present

legal approaches in systems for the protection of intellectual and industrial property "may be throwing up serious obstacles to the dissemination of information or to international trade in information, computer and communication services". The answer to that question, the paper declared, would "determine how far concerted intergovernmental action should be sought and what form it should take, to clear up any problems in that case, to define what stages could be contemplated on the way to more explicit rules for liability in the [informatics] technologies"<sup>19</sup>.

The danger of a mere review, the stretching of copyright legislation and its adaptation to the new technology is that the "mind-lock" of the old approaches may be imposed, with great inefficiency and even economic injustice, upon the liberating operation of the new technology. The information rich countries, and those with high investment in the production and extension of information technology, will reasonably require a just recompense from the information poor countries which seek ready access, by TBDF, to such information. The balance between these two competing forces is yet to be struck. But it seems likely to me that the technology itself, together with the current domestic and international mood of deregulation, may promote a breakdown in orthodox approaches to intellectual property law. It may lead to a demand for something fundamentally different in the adjustment between the information "haves" and "have nots".

## CONCLUSIONS

There are many other issues to be addressed in considering the impact of TBDF on the law. Some of the other issues were reviewed by me in a paper for the OECD in 1982<sup>20</sup>. Others have been reviewed in an important paper by Dr Peter Robinson<sup>21</sup>. Still more appear in the burgeoning material now being written on this important topic<sup>22</sup>.

The importance of the legal "fallout" of TBDF is obvious. The law can be a facilitator. But it can also be an impediment to efficiency. And efficiency is not everything. There are other values - such as human rights, democratic government, a peaceful and law abiding society and world, protection from wrong doing, just security for secrets, including legitimate business secrets, etc. These interests need to be protected and upheld. Technology does not exist for its own sake. It exists to enhance the environment of humanity and the happiness and the fullness of life, in that environment, of the life of the individual.

We stand on the brink of the Century of the Pacific. We have entered the age of mature technology. Bringing these two dynamic forces, with much potential for the benefit of humanity, together in harmony is the challenge. That the challenge is enormous is demonstrated by this paper. The problems of the interaction of a fast moving universal technology and slow moving and heterodox legal systems have been demonstrated. The basic problem is the lack of a meeting place and of institutions to develop, guide and stimulate international, effective and compatible laws on the

most pervasive technology operating in the world today. My hope as I approach PACIT 88 is that this institutional vacuum, once again called to notice, will be recognised and tackled. The key is there in the proposal of Mr Nakasone. Japan, approaching the apogee of its dominance of informatics, is uniquely well placed to take helpful initiatives which will benefit the Pacific rim - and the world. With great industrial and commercial power go great international responsibilities and obligations. For the sake of the orderly development of TBDF, the economic advancement of humanity and the preservation of important values in all of our societies, I hope that the institutional vacuum will at last be perceived and steps taken to fill it.

# FOOTNOTES

- \* President of the Court of Appeal, Supreme Court of New South Wales, Australia. Former Chairman, OECD Expert Group on Transborder Data Barriers and the Protection of Privacy (1978-80). Former Chairman of the Australian Law Reform Commission. Commissioner of the International Commission of Jurists. Trustee, Atwater Institute, Canada. Views stated are personal.
1. J Bazin, "Pacific Rim - Exciting New Frontiers for Lawyers" in CBA National, January 1988, 10.
  2. See e.g. J C Smith, "Aise and Oedipus : Ideas of the Self in Japanese and Western Consciousness" (1986) 20 UBCL Rev 341; M Yasaki, "Feeling and Reason as a Recurrent Topic of Legal Culture : A Response (1988) 22 UBCL Rev 185.
  3. Y. Nakasone, reported Mainichi Daily News, 11 April 1988, 1.
  4. N Savage and C Edwards, "Transborder Data Flows : the European Convention and the United Kingdom Legislation" citing "Communications and International Trade : A Symposium", 1982, Washington, 3 in (1986) 35 International and Comparative Law Quarterly 710, 713.
  5. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1981, Paris. See note (1985) 59 Australian Law Journal 683.
  6. G Tucker, "Present Situation and Trends in Privacy Protection in the OECD Area", unpublished restricted paper, OECD, April 9, 1988. (DSTI/ICCP/88.5)
  7. Lord Eldon in Hansard, Parliamentary Debates (House of Lords) 5 July 1983, col 509. Cited in Savage and Edwards, ibid, 714.
  8. Tucker, 18.
  9. Council of Europe, Study on New Technologies, 1987, 2.
  10. J Bing, P Forseberg and E Nygaard, "Legal Issues Related to Transborder Data Flows", Consultative document for the OECD (DSTI/ICCP/81.9), 1981, 57. See also T M Rankin, "Business Secrets Across International Borders : One Aspect of the Transborder Data Flow Debate" (1985) 10 Canadian Bus LJ 213, 235.
  11. D C Rowat, "Scandals Add to Pressure for Public Access Law" in Transnational Data Report, vol 4, 37 (1982).



12. Report of the Swedish Government Committee (SARK) "The Vulnerability of the Computerized Society : Considerations and Proposals", 1979.
13. J d O Brizada, Address at the Opening Session of the IBI World Conference on Transborder Data Flow Policies, reprinted Transnational Data Report, July 1982, 33.
14. See eg Ward v The Superior Court of California 3 CLSR 206 (Cal)(1972).
15. P Robinson "Legal Questions and Transborder Data Flow", Paper for the Swedish and Norwegian Societies for Computers and Law, January, 1982, unpublished. See also P Robinson, "Legal Issues Raised by Transborder Data Flow" in (1986) 11 Canada-USLJ 295.
16. See R v Gold [1988] 2 WLR 984 (HL).
17. Testimony of W L Fishman, United States Banking Committee, Subcommittee on International Finance and Monetary Policy, 9 November 1981, mimeo, 11.
18. See discussion. S Stern, "Computer Software Protection after the 1984 Copyright Statutory Amendment (1986) 60 Aust LJ 333. See eg P Brazil, "Infringement of Copyright and the Problem of 'Piracy'" (1987) 61 Aust LJ 12.
19. OECD, The Information Economy : Policies and International Consensus, Theme IIIT Improving International Rules of the Game, December 1987, 16.
20. M D Kirby, "Legal Aspects of Information Technology", mimeo, OECD, 1982.
21. See Robinson in 15 above.
22. See e.g. L J Damon, "Freedom of Information v National Sovereignty : The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems" 10 Fordham International LJ 263 (1986-87), K Golden, "Transborder Data Flows and the Possibility of Guidance in Personal Data Protection by the ITU", 6, Houston J of Int L 215 (1984); P E Cole, "New Challenges to the US Multinational Corporation in the European Economic Community : Data Protection Laws" 17 Int L & Politics 893 (1985); A P Miller, "Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information : An Introduction to the Arrival of the New Information Age" 20 Columbia J of L & Soc Problems 89 (1986); M J Farley, "Conflicts Over Government Control of Information - The United States and Unesco, 59 Tulane LJ 1071 (1985).