The John Marshall Journal of Information Technology & Privacy Law

Volume 11
Issue 2 *Computer/Law Journal - Spring 1991*

Article 2

Spring 1991

Legal Aspects of Transborder Data Flows, 11 Computer L.J. 233 (1991)

Hon. Justice Michael Kirby A.C., C.M.G.

LEGAL ASPECTS OF TRANSBORDER DATA FLOWS

THE HON. JUSTICE MICHAEL KIRBY, A.C., C.M.G.*

I. INTRODUCTION

The rapid increase in transborder data flows ("TBDF"), otherwise known as "informatics," has created a number of legal problems of high complexity. Of its nature, law tends to be related to a particular territorial jurisdiction. TBDF is a global phenomenon. It mocks legal jurisdiction, defies its effectiveness, and challenges its capacity to keep pace with the range and complexity of the problems presenting. Sometimes international cooperation leads to the "soft law" of guidelines, such as the influential Organization for Economic Cooperation and Development ("OECD") guidelines on privacy and TBDF. However, generally little is done. National laws are developed which are ineffective to deal with multinational issues. Worse still they may be inefficient. The need for harmonization and international approaches must be *stressed.* The urgent need for institutional solutions must be *emphasized.* This is illustrated by reference to instances of TBDF crime. This article discusses the legal issues raised by the use of modern technology to send information, such as personal or financial information, across international borders.

II. THE PRIVACY PHENOMENON

I came to this issue in an unusual way. In 1975 I was appointed the first Chairman of the Australian Law Reform Commission. That body was established by Act of the Australian Parliament to provide advice on the reform and modernization of federal law. After a change of gov-

* President, Court of Appeal, Supreme Court of New South Wales, Australia; Companion of the Order of Australia; Chairman, OECD Expert Group on Transborder Data Barriers and the Protection of Privacy (1978-80); Governor, International Council for Computer Communications (1984-present); Commissioner, International Commission of Jurists (1984-present). This article is based on a paper presented at Inter Comm 90, the Global Telecommunications Congress and Exhibition held in Vancouver, British Columbia on October 25, 1990.

ernment in 1975, and pursuant to an election pledge, the new government asked the Commission to study and report upon the need for legislation to protect privacy. Australia's highest court had held in 1934 that there was no common law right to privacy enforceable in the courts.[1] The request to examine Australia's laws on privacy made specific reference to the new information technology and the special dangers presented to privacy by the advent of computers linked by telecommunications.

Coinciding with this project, a number of national authorities and international agencies began proposing laws or guidelines for the defence of privacy in the age of informatics. The Nordic Council was amongst the first. A Canadian report was extremely influential.[2] Drawing on general statements of human rights which included reference to individual privacy,[3] the Council of Europe in 1980 adopted a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In an attempt to extend the developing principles on privacy protection towards intercontinental application and record keeping, the OECD in Paris in 1978 summoned an Expert Group to formulate guidelines. Because of the work I was doing in Australia on the development of national privacy principles, I was sent to this Expert Group as my country's representative. In due course, I was elected Chairman of the Expert Group. It developed guidelines which in September 1980 were adopted by the Council of the OECD in the form of a recommendation to member states.[4] Those states include the developed countries of Western Europe, North America, Japan and Australasia. After some delay, all member countries accepted the recommendation of the Council of the OECD. The Guidelines, therefore, became a basis of agreed action for the protection of privacy in the context of TBDF. Although the OECD recommendations were not binding, they have influenced the development of national and subnational laws and policies. In Australia, the Privacy Act 1988 schedules "privacy principles" which amount to an adaptation of the OECD guidelines. In Canada, the Canadian Privacy Act, with the complementary Access to Information Act came into force on July 1, 1983.[5] The Canadian Privacy Act affords rights to citizens and permanent residents to examine information about themselves under the control of federal institutions. It replaced and expanded provisions in the Canadian Human Rights

1. Victoria Park Racing & Recreation Grounds Co. Ltd. v. Taylor, 58 C.L.R. 479 (1937).

2. CANADA DEP'T OF COMM. AND DEP'T OF JUSTICE, PRIVACY AND COMPUTERS (1972).

3. *See, e.g.*, Universal Declaration of Human Rights, art. 12; International Covenant on Civil and Political Rights, art. 17; the European Convention on Human Rights, art. 8.

4. *See infra* pp. 240-41.

5. Can. Stat. 1980-81-82-83, ch. 111.

Act. The Canadian Privacy Act embodies the eight OECD principles. Those principles have also been adopted in Canada by private sector organizations.

The motivation for the preparation of the OECD guidelines was complex. Preparing quasi legal norms has not been a feature of the operations of the OECD. But with the rapid development of national and subnational laws for the protection of privacy, operating on the technological phenomenon of informatics (and specifically TBDF), it became apparent by the mid-1970's that a lack of consistency of approach would have adverse economic and social consequences. It might be impossible for those dealing in data to comply with different national laws in respect of data flows passing though (or accessible in) multiple jurisdictions. Further, the lack of consistent laws could lead to inefficiencies and inhibitions on the desirable flow of data or bureaucratic machinery designed to reconcile the incompatible legal obligations of data carriers and users. In this way, it was thought that if a general legal regime confirming basic guidelines could be laid down and followed in national and subnational laws and policies, the inefficiencies or at least gross inconsistency of regulation could be avoided. At the same time, the basic right to privacy could be upheld in multiple jurisdictions, notwithstanding the international nature of the technology from which the danger to privacy could sometimes arise.

It is in this way that a practicing judge, at home in the daily problems of the courts, became involved in the technology of informatics (the marriage of computers and telecommunications) and the intricacies of legal regulation of TBDF. An insight into the difficulties, and the urgent necessity of protecting the value of the privacy in TBDF, takes the rational mind to a consideration of other legal and social problems that present from this phenomenon. It raises the fundamental question of what organization will take initiatives similar to that which the OECD took in establishing guidelines for the protection of privacy. At a time when it is commonplace to boast of the triumph of the rule of law, it is a hollow boast if the law proves itself incompetent to tackle the myriad of problems presented from a source which is at once highly technological in nature and global in impact.

III. TRANSBORDER DATA FLOWS

TBDF may be broadly defined as the transfer of computerized data across national borders.[6] The data transferred by TBDF may be scientific, economic, technical or personal. The media may be ordinary text on microfilm, punched cards or computer listings transmitted by ordi-

6. Vrije Universiteit Brussel, Centrum voor Internationaal Strafrecht, *The Transborder Flow of Personal Data*, COMPUTER & LAW 3 (Oct. 1989).

nary mail. It may be in "machine readable form," such as the diskette upon which the hard copy of this paper was sent by mail to Canada. But it will generally be computerized data. This represents by far the greatest source of TBDF. Such data may be transmitted from a terminal to a computer system as part of an international network. The data are then processed in the system and sent back to the terminal. The data may be stored on line in a network directly accessible to anyone with a key to enter the system. Alternatively, it may be transported through telephone lines, specific data networks, by satellite, etc.

International transfer of data can take at least five forms.[7] First, it may be in the form of non-market flows, such as the domestic data passing through the computer network of a multinational corporation. Second, it may pass through market flows, such as a commercial flow arising from access to foreign data banks or a foreign data processing bureau. Third, it may be related to international transactions such as electronic transfer of funds ("EFT"). Fourth, there are data flows within a closed user group. Member banks, for example, use the SWIFT network. They pay a fixed price for every message. Access to the network is limited to members. Finally, there are operational flows including international transfer of software or data. These include the international remote maintenance of a system or the use of a backup system located abroad as security against accidents, terrorism, viruses or other sources of the vulnerability of informatics systems. Very many services today depend upon the international transfer of data. The most obvious cases are seen in the industries built on insurance, air transport, credit facilities and tourism. The modern international corporations could not operate without TBDF.

Increasingly large quantities of data flow across borders in the course of trade and industry. Several nations recognized this fact, and its obvious implications for the protection of privacy and the effectiveness of local laws to that end, led to early licensing legislation designed control the transfer of personal data on local citizens for automatic processing abroad. This was the effect of the Swedish Data Act of 1973. The idea was soon seized upon by Brazil as a means, less for the protection of the human rights of local citizens than for protectionism of local industry.[8] Hence the Brazilian government developed the policy on

7. *Id.*

8. 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

TBDF. There was a fear that such local regulation, enacted ostensibly for privacy protection, would in truth be aimed at economic protectionism. This fear was one of the stimuli that led to the initiative of the OECD to establish the expert group which developed its Privacy Guidelines. The spectre was presented that these national laws might unnecessarily impede the economically beneficial flow of data across national boundaries. Further, this could lead to a cacophony of laws which do little to advance human rights but much to interfere in the free flow of information and ideas.

In the development of the OECD Guidelines there was something of a tension between the viewpoints of the countries of Europe (with which Canada was more closely associated) and that of the United States of America. The continental countries of Europe had, within living memory, seen the misuse of files of personal data kept in hard copy form in folders. There was therefore a sensitivity to the practical necessity of protecting privacy and the imperative obligation to do so even in the case of a new technology which might keep and process the data outside the jurisdiction but provide for its retrieval within the jurisdiction. On the other hand, the United States, nurtured in attitude by the free flow of information guaranteed by the First Amendment to its Constitution, urged the primacy of the value of free data flows and the need to avoid unnecessary inhibitions upon them. It was perhaps only coincidental that the economic interests of the United States, as dominant in the technology of informatics, also favoured free flows; whereas the infant industries of Europe might be advantaged by local regulation.

The OECD Guidelines contain, at their core, eight basic principles to govern the protection of personal data in TBDF. These are:

1. The collection limitation principle: data should be obtained lawfully and fairly;
2. The data quality principle: data should be relevant to their purposes, accurate, complete and up-to-date;
3. The purpose specification principle: the identification of the purposes for which data will be used and destruction of the data if no longer necessary to serve that purpose;
4. The use limitation principle: use for purposes other than those specified is authorized only with consent of the data subject or by authority of law;
5. The security safeguard principle: procedures to guard against loss, corruption, destruction or misuse of data should be established;
6. The openness principle: it should be possible to acquire information about the collection, storage and use of personal data systems;

---

in Brazil. JDO Brazada, Address at the Opening Session of the IBI World Conference on Transborder Data Flow Policies, *reprinted in* TRANSNATIONAL DATA REPORT 33 (July 1982).

7. The individual participation principle: the data subject normally has a right of access and to challenge data relating to him or her; and
8. The accountability principle: a data controller should be designed and accountable for complying with the measures to give effect to the principles.

However, the OECD Guidelines also contain principles of international application. In paragraph 15, member countries were obliged to take into consideration the implications for other member countries of domestic processing and re-export of personal data. In paragraph 16, they were to take all reasonable steps and appropriate steps to ensure that TBDF of personal data, including in transit, are "uninterrupted and secure." Limits on the restriction of TBDF were accepted in paragraph 17. In paragraph 18, member States of the OECD were pledged to avoid developing laws, policies and practices "in the name of the protection of privacy and individual liberties which would create obstacles to [TBDF] of personal data that would exceed requirements for such protection."

The OECD has not rested on its laurels in this field where its work has been so influential. In 1985, a Declaration on Transborder Data Flows was accepted by which the member countries of the OECD acknowledged the importance of free TBDF, both for countries and for trading enterprises. The general principle of the free flow of information, the openness of policies on TBDF and the desirability of harmonizing national approaches were also accepted. In 1988, the OECD established a Commission for Computerized Information and Privacy. It envisaged revision of the guidelines in 1990. The advance of the technology of informatics has made some of the provisions of the 1980 OECD Guidelines questionable, or at least needing of consideration. The purpose specification principle, for example, may nowadays be readily circumvented by technological developments which permit searching of data for identifiers which were not specifically considered at the time when the data was originally collected. It is in this way that it is essential, in developing guidelines (still more legislation) to deal with information technology issues, to keep pace with the technological developments which constantly enhance and change in relevant ways the capacity of the technology.

IV. VULNERABILITY OF FINANCIAL INFORMATION

Privacy protection is but one concern presented to our societies by the advance of informatics. Another concern was discussed at an expert meeting held in Toronto in February 1990 under the auspices of a number of international banks, brought together by the Royal Bank of Canada. The experts examined the problems presented by the manipulation of information systems, sometimes with fraudulent intent, some-

times without intent to secure personal gain but with reckless indifference to the consequence of the conduct involved. A feature of the manipulation of TBDF has been the enormous damage that can be done, especially by the introduction of computer viruses. Cases include:

* The example of Robert T. Morris, Jr. who introduced a "worm" into information systems with consequences involving financial losses to those affected estimated to amount to $97 million. Some observers had condoned the activities of a brilliant student who demonstrated the inadequacy of computer security for protecting the data. Others regarded the conduct as seriously antisocial, requiring deterrent punishments and civil liability laws to make intrusions less attractive and to spread the burden of the losses caused by them. Mr. Morris was convicted under the Computer Fraud and Abuse Act (US); and
* In late 1989, thousands of personal computer diskettes were distributed, ostensibly with data about the AIDS virus. These diskettes contained a very serious "Trojan Horse." It disabled information systems into which they were inserted, allegedly for the purpose of extracting an extortion for the retrieval of the otherwise lost data. The alleged perpetrator of the offence was arrested in Cleveland (USA) on a warrant issued in London, England from where most of the diskettes were posted world-wide (although not to the United States and Canada). The diskettes were allegedly distributed for a Panama registered company. Although not involving international financial information directly, the case neatly illustrated the interjurisdictional character of many information offenses today.

There are many other cases which illustrate the inadequacies of substantive law to cope with new problems presented by information technology. One of the most notable is a decision of the English House of Lords in *The Queen v. Gold*.[9] An accused had secured access to data bases by using another person's access code and password. He was prosecuted for forgery under the Forgery and Counterfeiting Act of 1981. It was necessary to show that the accused had made a false "instrument." That word was defined to mean (amongst other things) "any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means . . . ."[10] The prosecution argued that the false instrument was the buffer in the computer containing the false information while it was being checked. The English courts disagreed. They were scathing of the "Procrustean attempt to force these facts into the language of an Act not designed to fit them. . ."[11] The judges urged that, if new legislation were to cover computers, it would need to "be better targeted." There are many like cases which illustrate the difficulty of applying the words of the common law

9. 2 All E.R. 186 (1988).

10. *See id.* at 189.

11. *Id.* at 191 (Lord Lane, CJ) (quoting 3 All E.R. 1987, 618 at 622-23).

or of statutes to new problems presented by information technology. Where those problems have the international character of TBDF, they are rendered even more difficult to solve.

At the Toronto conference on the vulnerability of international flows of financial information, it was recognized that even if deficiencies of substantive law definitions could be overcome, there are other practical problems in securing cooperation of law enforcement and private sector agencies over jurisdictional borders. The participants urged:

* The need to pool information on incidents and losses in order to disclose patterns of fraudulent transactions by repeat offenders;
* The need to cooperate in police and other training, including in specialized colleges in several jurisdictions;
* The need to recruit and pay at an appropriate level highly skilled police and other investigators to assist in the detection and prosecution of offenders having connection with a number of jurisdictions;
* The need to secure cooperation between common carriers and agencies providing telecommunication services and police and, if necessary, changes to the law, to permit (under appropriate conditions of confidentiality) the monitoring of electronic transactions to detect "hackers" and other persons engaged in information offenses;
* The need to enhance formal and informal cooperation between law enforcement and like agencies across jurisdictional borders; and
* The need to reform the law to increase the power of investigating agencies to cope with new problems presented by interjurisdictional offenses.

Any study of these issues requires consideration of the national laws that have been passed in an attempt to cope with manipulation of TBDF of financial data in connection with a number of jurisdictions. These national laws include:

* The need for the passage of "long-arm statutes" with purported extra territorial operation of one state's law in another legal jurisdiction;
* The negotiation of extradition treaties providing for the return of accused persons for trial on a wider range of offenses and on new principles of mutuality and reciprocity;
* The enlargement of formal and informal exchanges between law enforcement and like agencies;
* The negotiation of bilateral treaties to deal with particular offenses; and
* The reduction of disparities among new laws by the development of international guidelines designed to promote the harmonization of the expression of new data offenses.

The Toronto meeting emphasized the need for new initiatives, along the lines of the OECD Privacy Guidelines, to promote the harmonization of principles upon which future domestic laws for the protection of vulnerable TBDF of financial data could be modelled. A number of the participants thought that the OECD would be the most

suitable venue for intercontinental work of this character, relevant to the major players in the international data flows of vulnerable financial information. It may be hoped that the OECD will respond to repeated suggestions of this kind. A sign of hope that it may do so is the expression of personal opinion by Dr. H. P. Gassmann, a senior and highly experienced officer of the OECD that "the OECD could . . . be more used for rule-making."[12] Whilst emphasizing that this was a personal view, Dr. Gassmann certainly reflects opinions which were expressed at the meeting in Toronto and elsewhere. Unless an initiative is taken somewhere, the result is that nothing gets done. This reveals a major institutional gap in the strategy of addressing the problems posed by informatics and, particularly, by TBDF.

V. OTHER ISSUES

There are many other issues of a legal character presented by TBDF. Amongst the most urgent is the need for a new international regime to protect intellectual property in the context of informatics. Traditionally, intellectual property law was developed to provide protection to the medium rather than to 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 physical objects. 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. The question now posed is whether the old methods of protecting intellectual property are still apt means for achieving the appropriate social balance between inventors and users of information based systems in the age of TBDF. An added difficulty is provided by the fact that information produced in one country may be reproduced in ephemeral form in another. Unless arrangements can be made to recompense the original author in some way, the intellectual property in the idea will go unrewarded.

The recognition of this problem has led to the establishment of committees in UNESCO and in the World Intellectual Property Organization ("WIPO"). The OECD has also taken certain initiatives to ex-

12. Address by H.P. Gassmann: Towards Free Trade in Telecommunications and Information Services. Conference on the Future of World Telecommunications and Information Technology, May 2-3, 1990.

amine issues of intellectual property law in the context of TBDF. Some local laws have been enacted, including in my own country.[13] However, these have largely been stop-gap measures. They leave unanswered, particularly on the international stage, the more fundamental question of whether a more radical and novel approach is required for the protection of intellectual property interests because of the capacity of informatics and TBDF to divorce the medium and the message.

This is the fundamental question which an OECD paper has raised about the impact of TBDF on intellectual property law.[14] That paper said that the present legal approach may be "throwing up serious obstacles to the dissemination of information or to international trade and information, computer and communication services." The need to avoid the "mind-lock" of old legal approaches is presented by the phenomena of TBDF. All too often technology rushes ahead while the human mind—and one might say the legal mind in particular—remains for a decade, or more, captive to the technology of the past. There is nothing new in this. Surgery before the use of anesthesia depended upon the speed of the surgeon's performance. It was by such speed that the surgeon's skill was measured. It took more than a decade after the introduction of anesthesia as a regular feature of operative practice, for a change in such a time-honoured approach to the professional task.

If the OECD, or some other international agency might be expected to fill the "regulatory vacuum" on matters such as the impact of instantaneous TBDF on contract law, on the law of international insurance, on intellectual property law and on international vulnerability and data crimes, there are other issues which appear to lace any conceivable institutional venue. These include the relevance of TBDF to interactive freedom of information law, to the proof of matters in courts of law and tribunals by computer generated evidence, and even to the principles of conflicts of laws.

Those principles of conflicts of laws are accurately presented by the phenomenon of TBDF. An electronic message may be generated in country A. It may be switched in countries B and C. It may transit countries E, F, G, and H. It may then be processed in counties I and J, stored in country K and involve entities residing in and operating in other countries. Whose law applies to such TBDFs? Which law applies to data processing carried out by a computer on an orbiting satellite?

The OECD Guidelines on privacy urged that member countries of

13. Stern, *Computer Software Protection Under the 1984 Copyright Statutory Amendment*, 60 AUSTRALIAN L.J. 333 (1986); Brazil, *Infringement of Copyright and the Problem of Piracy*, 61 AUSTRALIAN L.J. 12 (1987).

14. OECD, *The Information Economy—Policies and International Consensus*, in IMPROVING INTERNATIONAL RULES OF THE GAME 61 (1987).

the OECD "should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data."[15] Following that well meaning but somewhat ineffectual plea, nothing much has been done to clarify the applicable private international law principles as they concern TBDF. The Hague Conference on Private International Law might help clarify the issue. But it tends to specialize in conflict of law problems applicable to international sales of goods. The more conceptual issue of developing an effective international legal regime to determine the law, civil and criminal, applicable to such movements of data, remains for the future.

VI. THE INSTITUTIONAL ISSUE

The advent of informatics and TBDF has produced an extraordinary revolution with enormous implications, not only for the economies of every country, but also for world peace, interdependence and security. In 1985, before perestroika and glasnost arrived in the Soviet Union, the United States Secretary of State, Mr. George Schultz, in a speech to the National Academy of Sciences said:

> The free flow of information is inherently compatible with our political system and values. The Communist States, in contrast, fear this information explosion perhaps more than they fear Western military strength. If knowledge is power, then the communications revolution threatens to undermine their most important monopoly . . . their effort to stifle their peoples' information, thought and independence of judgment. Totalitarian societies face a dilemma: either they try to stifle these technologies and thereby fall further behind in the new industrial revolution or else they permit these technologies and see their totalitarian control inevitably eroded.[16]

This is the reason why, until recently, photocopiers in the Soviet Union were locked up, why direct dialling was impossible and telephone books unavailable. It explains why the leaders of liberal thought in Eastern Europe and China made constant contact with sources of ideas and encouragement outside their beleaguered lands through telecommunications, facsimile and, increasingly, interactive computers. The global network of informatics is a great force for liberty because it renders every corner of the world interdependent, it is also a great force

15. Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, OECD 12 Paris (1981).

16. Quoting address by H.P. Gassmann: New Communications Technologies in the Global Information Age—Policy Challenges and Social Implications, Ohio State University 1, Apr. 3, 1989.

for peace and security.[17]

But an invader from Mars would not believe the shocking neglect of the institutional and legal issues presented by TBDF. TBDF is an amazing technology of enormous potential in so many ways. Yet the world has seen its advent without developing, in the twenty-five years of the advance, any effective global institutional responses. True, the OECD has done some valuable work. There have been useful national enquiries on particular subjects. Private institutions and universities have done useful research. But a coherent doctrine of TBDF law and policy has simply not developed. It is amazing to me that such a valuable economic commodity has not produced its own servicing institutions, if only to reduce the inefficiencies which will result from the failure to develop internationally accepted principles. The consequence will be either: the chaos of a multitude of voices speaking to a truly intercontinental phenomenon; a failure to act with the consequent erosion of important and hitherto protected rights; or the over-reach of the law of the information powerful to govern the rights and duties of those in the information poor.

We are living through a time which, in many ways, has hopeful portents for individual liberty and economic progress. But it is not much use boasting about the final ascendancy of the rule of law if, in the face of an expanding international technology of the greatest importance, our law is out of date, irrelevant, inapplicable or, worse still, silent. In that realm of inadequate law or of lawlessness, the law of the jungle is substituted for rational rules of international application. An international technology should be better served by international institutions and international rules of the road. What is needed is quite simple. In the face of the phenomenon of TBDF we need well funded private sector research and investigation to stimulate the development of basic rules which may be accepted by international agencies and national governments. We also need a new initiative by international bodies addressing the many legal issues posed by TBDF. The OECD Guidelines on Privacy showed the way. It is a pity that the momentum built up in that most practical of international agencies in 1980 was lost. It is to be hoped that the momentum can be rekindled both in the OECD and in other agencies with relevant missions. Sensitivity to human rights and to the needs of developing countries is imperative. But for those unimpressed by humanitarian concerns, the sheer inefficiency of regulating an international technology by a multitude of diverse national laws should afford a sufficient spectre to promote international cooperation and effective institutional responses. In a way

17. *See* Armstrong, *Foreword* to TELECOMMUNICATIONS LAW: AUSTRALIAN PERSPECTIVES (1990).

that transcends technological issues, this is a fundamental question posed for all of our countries by this meeting of Inter Comm 90.

REFERENCES

M. ARMSTRONG, TELECOMMUNICATIONS LAW: AUSTRALIAN PERSPECTIVES (1990).

Branscomb, *Rogue Computer Programmes and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL 1 (1990).

Brazil, *Infringement of Copyright and the Problem of Piracy*, 61 AUSTRALIAN LAW JOURNAL 12 (1987).

Canada, Department of Communications and Department of Justice. 1972, *Privacy and Computers*, Govt. Printer, Ontario.

Forum on the International Legal Vulnerability of Financial Information, February 26-28, 1990 Toronto, Canada, Summary Record and Statement. (Mimeo).

H.P. Gassmann, *Towards Free Trade in Telecommunications and Information Services*, Address to Conference on the Future of World Telecommunications and Information Technology, New York, May 2-3, 1990, (mimeo).

H.P. Gassman, New Communications Technologies in the Global Information Age—Policy Challenges and Social Implications. Lecture at Ohio State University, April 3 1989, (mimeo).

M. Kirby, *Legal Aspects of Informations and Transborder Data Flows* in ESSAYS ON COMPUTER LAW, 197 (G. Hughes ed. 1990).

Organisation for Economic Cooperation and Development, 1981. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (1981).

Organisation for Economic Cooperation and Development, 1987. The Information Economy—Policies and International Consensus. *Improving International Rules of the Game*, 61 OECD (1987).

Vrije Universiteit Brussel, Centrum voor Internationaal Strafrecht, Computer and Law: *The Transborder Flow of Personal Data*, (October 1989) (mimeo).

Stern, *Computer Software Protection Under the 1984 Copyright Statutory Amendment*, 60 AUSTRALIAN LAW JOURNAL 333 (1986).