SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Canada-United States Law Journal

Volume 11 | Issue

Article 32

January 1986

Legal Issues Raised by Transborder Data Flow

Peter Robinson

Legal Issues Raised by Transborder Data Flow

*by Peter Robinson**

INTRODUCTION

This paper deals with legal issues raised by transborder data flows (TBDF) in the broad international context with illustrations from the more narrow Canada-U.S. context. It will attempt to step beyond the question of privacy protection, which, while important, is by no means the only legal issue arising from TBDF. It has, however, received prime place for many years even to the exclusion of other legal issues in international meetings.

The current situation has recently been encapsulated by Edward Ploman:

> Part of our dilemma is linked to the fact that existing legal rules and regulations are stretched beyond their inherent capacity to cover new situations. Trade law can manage shoes and cars but not information. Copyright law is in a mess faced with the rapid introduction of new information processes and products. We seem to be marching ahead with our faces turned towards the past and our backs to the future.[1]

The main thesis of this paper is that many TBDF issues arise because a user of TBDF is operating, virtually simultaneously under two (or more) different legal and jurisdictional regimes. The resulting implications suggest some difficult times ahead unless a concerted effort is made now to begin to understand the requirements.

WHAT ABOUT DEFINITIONS?

Increasing attention is being given to legal questions raised by TBDF, but those questions, must be better defined before they can be adequately tackled. Most lawyers prefer to start with a series of definitions. For example, Anne Branscomb, after a brief introduction, launches into a discussion of definitions in her paper entitled "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition."[2] In a report entitled "Legal Problems related to Transborder Data Flows,"[3] authors *Bing et al.* provide a discussion on the

* Canadian Department of Communications. Former Chairman, OECD Working Party on Transborder Data Flows.

[1] Edward Ploman *quoted in* 8 TDR: TRANSNATIONAL DATA REPORT, at 401 (Dec. 1985).

[2] Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flows in Transition*, 36 VAN. L. REV. 985, 990 (1983).

[3] AN EXPLORATION OF LEGAL ISSUES IN INFORMATION AND COMMUNICATIONS TECHNOLO-

definition of a number of basic terms, such as "telecommunication," "telegraphy," "broadcasting," "mail" and "information." The need for definitions is so ingrained that Mr. Justice Kirby, in his presentation to the first session of the Organization for Economic Cooperation and Development (OECD) Committee for Information Computer and Communications Policy (ICCP), devoted some early words to "starting without definitions."[4] I intend to substantially follow that lead while recognizing that an important part of the problem is definitional. At the same time, I begin to question the desirability of a narrow definition because with the rapid changes in technology, definitions may become quickly outdated.

Initially there is need to circumscribe what is meant by transborder data flow. The following working definition is used:

> The transfer of data and/or information across national borders, usually (although not always) in machine-readable form, and usually (but not inevitably) over telecommunications facilities.

This "definition" attempts to exclude, in general, communications via telephone, ordinary letter mail, and radio and television, and puts emphasis on information required for business operations.

The problem with this (or any other) definition of TBDF is that it places emphasis on the act of transfer of the data while most of the issues do not directly relate to the transfer. This focus has caused a great deal of confusion in the past, because attention is diverted away from the real issues such as privacy protection, trade principles, employment, etc. Only in recent years with the general acceptance that TBDF issues have little to do with "flow" per se has much of this confusion disappeared.[5]

Another basic definitional question is: what does "legal issue" mean? This is not an esoteric question such as, "how many angels can stand on the head of a pin?" The question has a great deal to do with how the issues are tackled. I have previously asserted that legal issues are secondary[6]—not in terms of complexity, nor in terms of importance—in the sense that they arise after the substantive issues have been defined, or when legal approaches are considered as a means of resolution. I am not sure whether lawyers feel that this "secondary" position denigrates the legal profession, but it has not yet been accepted. (Indeed, I was persuaded to change my attitude on this point for a while, but have now reverted to my earlier position.)

GIES, (ICCP Series No. 8) (OECD Paris 1983) [hereinafter cited as *ICCP*]; J. Bing, P. Forsberg & E. Nygaard, Legal Problems Related to Transborder Data Flows 63 (unpublished manuscript) [hereinafter *Bing*].

[4] *See ICCP, supra* note 3; *Bing, supra* note 3; Kirby, Legal Aspects of Information Technology 14 (unpublished manuscript) [hereinafter *Kirby*].

[5] *See, e.g.*, Robinson, *TDF: The Hardy Perennial*, TELECOM. POL'Y 272 (Dec. 1983); Montgomery, *Transborder Data Flow: Canadian Directions*, in TRANSBORDER DATA FLOWS: PROCEEDINGS OF AN OECD CONFERENCE 71 (North-Holland 1985) [hereinafter *Montgomery*].

[6] *See, e.g.* Robinson, *Transborder Data Flow—A Canadian Perspective*, 2 INFORMATION PRIVACY 57 (Mar. 1980) [hereinafter *Canadian Perspective*].

One might also argue that a legal issue is one that deals with law, or one which interests lawyers—but both of these approaches are tautological and are of little help. Some cynics have suggested that a legal issue is one from which lawyers can make money: and it can certainly be expected that lawyers will have a field-day in dealing with growing tensions and legal conflicts in the TBDF area. It would perhaps be unfortunate if it was felt that a legal issue was one which inevitably resulted in new legislation. If this were the case, many countries would avoid dealing with issues until sufficient case-law was established. With the rapid pace of technological change, and growing interdependence among nations it is questionable whether this is an effective way of proceeding.

Most of my legal friends—presumably because of professional pressures to deal with specifics rather than with hypothetical questions—are uncomfortable when dealing with concepts. Practicing lawyers are concerned with the existing legal structure, and are primarily interested in assisting their client (or employer) accomplish what he wants within that structure. The corporate lawyer's main concern, is therefore, to adapt to the legal structures in which his firm and its affiliates operate. New legislation could give him additional headaches, and in particular, he will be opposed to any legislation which raises barriers to, or restrictions in achieving corporate objectives. He is less interested in hypothetical questions of the "what if. . .?" variety. But questions of this type are particularly important, because of the difficulties which the law is now having with data and information.

The Underlying Source of TBDF Issues

As I have already stated the underlying source of many TBDF issues is that a user of TBDF is operating under two (or more) legal and jurisdictional regimes. It is clear that government objectives in these two legal environments are not only likely to differ, but may even be in conflict, particularly, for example, if they concern competing for and attracting high technology activities (including employment) to their territories. There are then likely to be conflicting demands on individuals and corporations in regard to their use of telecommunications and computing facilities and services. Part of these conflicting demands inevitably include conflicting legal requirements.

Issues arise, based on the fact that:

> The very technology which has linked computers by telecommunications renders law, 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.[7]

Pressures will mount to deal with the difficulties which arise from conflicting legal requirements, and which will increasingly be seen as limitations on exchanges of data and information, and barriers to growing international trade in services. Demands will increase for greater harmonization, or at least compatibility, in the legal approaches adopted by different governments. At issue will be the extent to which a government may change its policies in order to accommodate foreign pressures. With regard to the United States, for example, it has been asserted that: "The United States political system, peculiar to itself, will prevent the modification of its institutions to harmonize with the rest of the world."[8]

This statement was made in 1979. With the pace of technological change, and with the progress made in understanding trends and concerns, it may no longer be true; yet, in my own experience, I often see indications that it might be. Indeed, I get the impression that some in the United States feel that "those who are not with us are against us"—a sentiment which leaves little room for healthy and honest disagreement and makes harmonization, or even compatibility, through compromise extremely difficult.

The author of that assertion went on to state that:

> I will be surprised if the United States does not sacrifice the economic advantages of free flow of information to the political necessity of passing the sort of laws that suit its domestic needs;[9]

and concluded:

> The country which most eagerly seeks to ensure the free flow of information internationally will prevent the making of the international agreements necessary to secure this goal.[10]

Perhaps these views are exaggerated, but it is clear that all countries, including the United States—and Canada—would like to see international agreements mirror their own legislative approaches for dealing

---

[7] *See Kirby, supra* note 4, at 12.

[8] Norman, *Compatibility, Harmonization and Interworking—The Future of Open International Systems*, in COMMUNICATIONS, INFORMATION PROCESSING AND THE PRODUCTIVITY REVOLUTION 64 (1979).

[9] *Id.* at 79.

[10] *Id.* at 64.

with TBDF issues. Many sensitivities will be touched as pressures mount from foreign sources to modify legislation. How far any country will bow to those pressures will depend on many factors, and concern about the extent to which a country will be expected to modify its legislation and its policies in order to accommodate a larger developing consensus will increase. One might look at the current United Kingdom approach for dealing with privacy protection as a possible example of such modification. Their approach appears to differ from traditional approaches in Common Law and moves closer to traditional European approaches.

In general there will be reluctance to adopt the unaltered approach of another country. To do so in some circumstances could give advantage to industry in that second country, for example. Or perhaps the change will create anomalies with other existing domestic legislation.

While problems are likely to arise with existing legislation, there will be need to avoid perpetuating those difficulties in new laws. As new legislation is contemplated, efforts will be required to develop compatible approaches, rather than to cater solely to domestic situations and requirements. This has already been done in the case of privacy protection, with the OECD Guidelines,[11] and the Council of Europe Convention.[12] Similar exchange of views has occurred with regard to computer-related crime,[13] and further efforts in other areas will be necessary if escalating friction and confrontation are to be avoided.

FREE FLOW

Considerable confusion has arisen regarding interpretations to be put on "free flow" of data and information.[14] Initially, many seemed to feel that it meant a "free for all" in which users of TBDF could do whatever they wished, without regard to the consequences. Such an interpretation is, of course, not generally acceptable.

All countries, no matter how large, nor how liberal and open they perceive their policies to be, are concerned about data and information which cross their borders. There were previous laws dealing with libel, slander, and incitement to racial hatred. Laws for consumer protection were established to guard against false advertising and laws were established to protect trade secrets and intellectual property. Subsequent laws deal with the protection of personal privacy—the issue that first drew attention to concerns over TBDF—and the issue which generated the "free flow" slogan when it was recognized that such protection would

[11] OECD, PARIS, GUIDELINES ON THE PROTECTION OF PRIVACY AND THE TRANSBORDER FLOWS OF PERSONAL DATA (1981).

[12] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Strasbourg (1981).

[13] OECD, COMPUTER RELATED CRIMINALITY: ANALYSIS OF LEGAL POLICY IN THE OECD AREA, Directorate for Science, Technology and Industry (Sept. 1985) [hereinafter Directorate].

[14] Robinson, *Transborder Data Flows: An Overview of the Issues*, in TRANSBORDER DATA FLOWS: PROCEEDINGS OF AN OECD CONFERENCE 17 (North-Holland 1985).

affect flows of data and information. All governments, then, in one way or another exercise control over data and information flowing across their borders. There is no such thing as a total "free flow" of all data and information.

My challenge to the "free flow" slogan was intended to draw attention to the fact that there were many important issues raised by TBDF—beyond the personal privacy issue—and which could not be dealt with by a simplistic "free flow" approach. My motives were interpreted as protectionist and other "signals" from Canada were also interpreted as indicative of a growing protectionist sentiment.[15] One of these "signals" was the Canadian Bank Act of 1980.[16] A report of the United States House Committee on Government Operations suggested that it:

> includes major and crippling limitations on the operations of foreign (i.e., U.S.) financial enterprises and on service providers . . . .[17]

An Assistant Secretary of the U.S. Treasury, in testimony before a subcommittee on the House Committee on Government Operations, later stated that:

> We have examined the provisions of the Canadian Bank Act carefully and are in close contact with the U.S. banking community. We understand that no American bank is experiencing serious difficulties as a result of these provisions.[18]

Unfortunately, the first of these comments was always remembered and quoted. Even today, it is uttered from time to time, but I believe that few people accept it as a valid statement on the Bank Act.[19] We are now beyond the stage of pointing accusing fingers at each other (for fingers can be pointed in the other direction too), we are at last listening to each other and trying to understand what is being said.

If issues raised by TBDF generally have little to do with flow, and if

---

[15] The report of the Canadian Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty, [hereinafter *Clyne Report*], perhaps cause the most consternation among U.S. business and government representatives. This was a report from an advisory group of knowledgeable people from the private sector, not the Canadian government.

[16] Paragraph 157 of the Canadian Bank Act of 1980 deals with the question of records maintenance. It requires that banks operating in Canada maintain within Canada, a certain minimum set of records of the transactions of its clients in Canada. Once this minimum requirement has been met, the data may be exported for further processing or parallel storage. (*See, e.g.* Robinson, *Transborder Data Flow: A Focus on Trade*, in THE MANAGEMENT OF TRANSBORDER DATA FLOWS: U.S.-CANADA AND BEYOND 84 (1984).

[17] U.S. HOUSE COMM. ON GOV'T OPERATIONS, H.R. REP. 1957, *97th* Cong., *1st* Sess. 7 (May 1981).

[18] *U.S. House Gov't Information and Individual Rights Subcomm. of the Comm. on Gov't Operations* (statement of Honorable Marc E. Leland, Assistant Secretary of the Treasury) TREASURY NEWS (Dec. 9, 1981).

[19] *See, e.g.*, Hugh Donaghue, Sectoral Free Trade in Computer Services (Apr. 1, 1984) (an unpublished presentation to the Brookings Institution) in which Donaghue states, "The actions of the Canadian government with regard to access and availability of data to their bank regulators is absolutely legitimate."

"free flow" is therefore not the issue it was once thought to be—particularly in the Canada-U.S. context, where our telecommunications networks are so closely integrated—what are the real issues?

The Canadian keynote speech[20] presented at the OECD Symposium on TBDF in 1983 indicates where we thought some of the more important issues lie, and subsequent events appear to confirm our view. Some of the particularly important issues identified in that paper are:

— The international telecommunications infrastructure;
— Trade in telecommunications and computing services; and
— Extraterritoriality.

I shall deal with these, and other, aspects below. In the following discussion, I have merged the first two items—i.e. telecommunications infrastructure and trade—because the two are so closely interrelated. Trade in services considerations cannot be divorced from the international telecommunications infrastructure. It does not automatically follow, of course, that all (or indeed any) telecommunications services in each country must be open to competition. This is an important point to understand, and to accept, if sensitivities are to be overcome.

TRADE IN SERVICES

A major focus of the international debate on TBDF would be trade in information-based services.

A first step in confronting these issues was the OECD Declaration on Transborder Data Flows.[21] It was welcomed in an official U.S. press release as "an important accomplishment by the OECD in the area of trade in services."[22] It recognizes the benefits from TBDF and, in it, OECD member governments declared their intention to:

a) Promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;
b) Seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows;
c) Develop common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonized solutions;
d) Consider possible implications for other countries when dealing with issues related to transborder data flows.

Preambular paragraphs in the Declaration indicate some of the concerns which have arisen, and recognize that policies affecting TBDF "reflect a

---

[20] *See Montgomery, supra* note 5.

[21] OECD, PARIS, DECLARATION ON TRANSBORDER DATA FLOWS, Press Release A(85)(30), (Apr. 1, 1985).

[22] UNITED STATES MISSION press release to OECD, UNITED STATES SUPPORTS OECD ADOPTION OF DECLARATION ON TRANSBORDER DATA FLOWS (April 10, 1985).

range of social and economic goals, and that governments may adopt different means to achieve their goals."

Much of the earlier confusion and rhetoric about TBDF evaporated after release of that Declaration. Out of a general morass of views and sensitivities, we were able to develop a clear sense of direction. What still remains unclear is just how we will be able to proceed in that direction; what specific steps need to be taken; where priorities lie; and what compromises will be necessary to maintain international cooperation. I hope that the OECD Working Party on TBDF will be able to achieve agreement on these points.

One aspect that will require close attention in all countries is that of telecommunications regulation. So far, regulatory measures have stemmed primarily from domestic requirements. It is now clear that foreign and international action in the telecommunications area can have significant domestic implications, and that such actions and international trends must be factored into telecommunications policy-making and regulation. Domestic telecommunications policies can no longer totally ignore international developments. This fact will create unfortunate dilemmas for politicians as they try to balance domestic social requirements against international economic pressures.

In particular, telecommunications regulation will inevitably affect comparative advantage in international trade. Such effect could disadvantage domestic industry as well as foreign industry. For example, the recent NTIA report entitled "Issues in Domestic Telecommunications: Directions for National Policy" gives a number of recommendations on regulation. In particular, it identifies several rulings of the AT&T Consent Decree which adversely affect U.S. industry, such as the one limiting overseas activities of the Bell companies.[23]

So far, much of the international debate on telecommunications regulation has centered on "monopoly vs. competition" as a part of the fallout from "de-regulation" in the United States, but it is becoming clear that the real issues lie elsewhere. I find the current "monopoly vs. competition" debate about as useful and informative as the earlier "free flow vs. restriction" debate. Those on the "competition" side of the debate recognize, I feel sure, that some telecommunications services will continue to be provided on a monopoly basis for some time to come in most countries. This will have to be factored into any international agreement affecting telecommunications. Those on the "monopoly" side of the debate must equally recognize the inevitability of increasing competition,[24] at least internationally. Recognition that the situation is not "black" or "white" will help to reduce current sensitivities in this debate, so that we may address more practical matters, such as the impacts of regulation on

[23] National Telecommunications and Information Administration, U.S. Department of Commerce, Issues in Domestic Telecommunications: Directions for National Policy 178 (1985).

[24] Robinson, *Telecommunications, Trade and TDF*, 9 TELECON. POL'Y 313 (Dec. 1985).

trade. In any case, governments must make assessments in their own interests if negative impacts on their own domestic industry are to be avoided.

Another important aspect of the debate on trade in information-based services will be "rules of the road" for access to data and information and related services. This was flagged in the Canadian keynote speech in the London symposium on TBDF,[25] and picked up in the OECD Declaration. Substantive work has already been done as far as personal data and privacy protection are concerned. The OECD guidelines[26] and the Council of Europe Convention[27] have dealt with the issues in terms of privacy requirements, not in terms of regulations on flow.

A 1984 conference of experts in Bellagio[28] considered the question of whether further creative work was necessary. One participant was of the view that:

> Data protection has reached a plateau, a time for consolidation and reassessment. It is now fully accepted as a necessary feature on the legal and institutional landscape: the last few developed countries are just joining the club. The enthusiasm of the early pioneers has become transmuted into the steady job of learning how to make data protection work—and how well it works still varies from place to place.[29]

Others were not quite so confident:

> This assertion evoked a number of valuable comments. There are considerable risks, it was pointed out, of an event or occurrence changing the current positive direction of data protection, such as new outbreaks of terrorism or a return to a negative economic situation. It was also noted that the anti-regulatory movement was growing in force in Western countries.
>
> The most pointed criticism of the above statement took exactly the opposite position and argued that data protection had reached not a plateau, but a slippery slope.[30]

It is clear that some concerns remain. For example, choice of law questions will probably be with us for a long time but there appears to be no pressure for their early resolution. Another question is whether measures should apply to protection of the privacy of "legal persons." There is a divergence of opinion on this point among OECD countries, but specific problems do not appear to have arisen and there are no strong pressures which necessitate full agreement at this point in time. It seems that meetings of Privacy Commissioners are covering operational issues, and

---

[25] *See Montgomery, supra* note 5, at 71.

[26] *Supra* note 11.

[27] *Supra* note 12.

[28] Flaherty, *Nineteen Eighty Four and After: The Final Report of the Bellagio Conference on Current and Future Problems of Data Protection (Apr. 9-13, 1984).*

[29] *See id.* at 13.

[30] *Supra* note 28.

no new major issues are arising. Therefore, the question of "rules of the road" for access to personal data appears to have been adequately dealt with for the time being, but, there are a few loose ends which may need attention in the future.

Another area that has been examined in the OECD is computer-related crime.[31] In spite of some differences in attitudes and in perceived needs, there was general agreement among members of the OECD expert group that current legal systems do not adequately deal with "computer crime," however defined. For example, misuses of computers may leave no physical trace, whereas existing law in general requires evidence of interference with or damage to some physical entity. Forgery provisions, in general, do not deal with representations in a machine and generally require representation on paper. In many countries, the crime of "fraud" is defined as deception of a person, not of a machine. Other questions arise regarding unauthorized acquisition of data from a computer system (which in some respects might be equated to "wire tapping"), unauthorized use of computer systems, or unauthorized acquisition of data from a computer. Some legal systems deal with some aspects of these actions, but most do not.[32] While full agreement has not been reached in this area, useful progress has been made. It is likely that further progress can only be made in a different international organization—probably one more closely associated with legal issues.

This is as far as the "access-to-data" work has progressed, but other facets of this issue are also important—and possibly of even greater economic importance. It has become clear that telecommunications and computing services are essential to the operations of business, and that action that severs access to essential data—particularly data that have already been used on a regular basis—will have adverse, and possibly serious, effects on corporations requiring that access.

Industry will then be reluctant to store data in a country where there is risk of the government barring access to those data at some future time. Governments, too, will wish to ensure that data essential to the operations of domestic industry, and which are stored abroad, are available on an "as required" basis. Without such a guarantee, there will likely be difficulty in reaching international agreement on trade in data-related services.

The example of Dresser (France)[33] brought this issue into public view: earlier suggestions I had made that such an event could occur[34] were dismissed as rhetoric. In that case, Dresser (France), a subsidiary of Dresser Industries in the United States, overnight, denied access to the computer which stored the latest specifications for manufacturing pipe-

---

31 *Supra* note 13.

32 *See, e.g.,* Canadian Criminal Law Amendment Act of 1985, 19 Can. Stat., 1985.

33 *See, e.g., Waging a Trade War Over Data*, N.Y. Times, Mar. 13, 1983.

34 *See Canadian Perspective, supra* note 6, at 57.

line equipment. The French subsidiary was, as a result, unable to manufacture equipment for the Siberian pipeline, and it lost a $3 million Australian order as well. Prior consultation before such action is taken in the future may be demanded in trade negotiations.

I have also suggested[35] that labor unrest could also lead, through strike action, to a denial of access to needed data-related services. Will unions be willing to guarantee essential services to foreign users in the event of a strike, provided, of course, that similar strike action has not been taken in that foreign country? Is there an alternative way of dealing with this requirement?

Another aspect of the access-to-data issue arose in a case involving a Canadian bank.[36] In this case, the Miami branch of the Bank of Nova Scotia was served with a U.S. grand jury subpoena demanding the production of information held in the Bank's branches in the Cayman Islands and the Bahamas. The Bank was unable to comply because the information requested was protected by the laws of these Caribbean countries. An application to the Cayman Islands courts seeking permission to release the information resulted in an injunction. In spite of this, the U.S. courts, supported by the U.S. Department of Justice, imposed a fine on the Bank of $25,000 per day until the information was produced.

> In attempts to resolve the problem, [t]he Canadian Government, both in diplomatic exchanges and in *amicus curiae* briefs, asked what the U.S. attitude would be if the government of a Middle Eastern state in which [the Bank] maintains an office issued an order, including sanctions, requiring the Bank to disclose information concerning the alleged business relations between a customer of its Miami office and Israel. For the Miami office to supply that information would violate the foreign political boycott provisions of the U.S. Export Administration Act of 1979, and would place the Bank in a situation of irreconcilable commands.[37]

This case, which on the surface appears to be legal, but which is perhaps more political because it concerns differences among governments, subsequently led the government's concern to pursue cooperative rather than confrontational avenues for dealing with such international judicial differences. President Reagan and Prime Minister Mulroney signed a Mutual Legal Assistance Treaty in criminal matters in Quebec on March 18, 1985. The U.S. also negotiated an arrangement for exchange of information with the United Kingdom on behalf of the Cayman Islands; Canada is involved in similar negotiations. Both Canada

---

[35] *Supra* note 6.

[36] *See, e.g., Scotia Bank Caught Between Two Sets of Laws*, The Citizen, Ottawa, Nov. 16, 1983.

[37] J. Fried, *Conflicting Assertions of National Jurisdiction Over Information Matters* 3, (presentation to the Media and Communications Law Section of the Canadian Bar Association) (Oct. 1984) [hereinafter Fried].

and the United States are each negotiating with the Bahamas for similar treaty arrangements. Surely there is a moral here somewhere!

This case gets down to the core of what I believe to be a cause of future friction and confrontation—foreign pressure to change domestic law. It seems logical to suggest that if an existing law aids and abets international criminals (for it was a criminal case that led to the demands for the protected information), then some change might be desirable. But if that suggestion comes from a foreign source, it is likely to touch on sensitivities and raise immediate opposition.

Is the solution to this particular issue an extension of the area covered by the privacy guidelines? Does it require further debate about international co-operation on computer crime? Is it a matter for trade agreement if the issue is defined more broadly? What is an appropriate international forum for looking into these question or is it merely a matter for bilateral agreement?

I believe that the access-to-data question is one which is beginning to demand more immediate attention. It does not yet have to be a part of trade negotiations, which present a confrontational environment. Indeed, it may be better to deal with this question elsewhere, such as in the OECD, which primarily is a consensus-building body. The OECD, of course, does not include the Caribbean countries and, as I have recently stressed,[38] there is a need to establish a forum for consensus-building which would include developing countries as well as OECD countries.

In addition to this new principle for trade in data-related services, the old principles developed for trade in goods must be assessed for their applicability to services. In this paper I will not go through all of these principles, but I would like to mention the "national treatment" principle. There are some difficulties in applying this principle without modification to data-related services. Some of these difficulties arise from the fact that the telecommunications system is the distribution system for such services. A country which provides greater ease of access to that distribution system may feel that it is offering greater opportunity for foreign trade in those services to industry from a country with more restricted access to the distribution system than is offered to its own industry in the other country. Again, foreign pressures are likely to demand policy changes in telecommunications, which is also highly sensitive to competing domestic pressures of a social and political nature. The principle of "most favored nation" (MFN) runs into similar difficulties.

Perhaps, as Rodney Grey is now saying,[39] we are not properly ap-

[38] P. Robinson, *The International Debate on TBDF: The Missing Link* 1, (presentation to TIDE 2000, the first of three seminars commemorating twenty years of Japanese membership in the OECD).

[39] R. de C. Grey, The Services Industries: A Note of Caution about the Proposal to Negotiate General Rules about Traded Services, (paper presented to a Research Symposium on the GATT and Canadian Interests, held by the Royal Commission on the Economic Union and Development Prospects for Canada) (Dec. 1983).

proaching the services question. Because of these sensitivities, I agree that expectations for rapid agreement on trade in services should not be too high. I am, however, not as pessimistic as Grey. Indeed, I believe that progress can be made in regard to international agreement on services related to data and information. Progress in this area is necessary whether or not discussions take place in the context of trade. I am convinced that if the trade people ignore these issues, they are sufficiently important to be picked up elsewhere.

EXTRATERRITORIALITY

Extraterritoriality—the reach of one country's laws into the territory of another—is one aspect of the concerns over impacts of TBDF on national sovereignty.[40] Other sovereignty concerns exist and will have to be addressed. Here, however, I have limited my consideration solely to the extraterritoriality question, since a number of the other concerns tend to be rather emotional (but no less important) and, therefore, somewhat less tractable.

The extraterritorial application of one country's laws within the territory of another is not a new problem, and has been raised under a number of different labels: conflicts of jurisdiction, conflicting legal requirements, or simply "ET." It has been stated that: "In even more simple terms, it usually refers to the application of American law outside the U.S.A."[41] While the problem may not be new, we can expect increasing use of TBDF to exacerbate the problem and perhaps add new twists.

Defensive legislation to counter the effects of the extraterritorial application of U.S. laws has already been passed by a number of countries, which include the United Kingdom, France, Australia, Norway and Denmark. The earliest legislation is the Ontario Business Records Protection Act of 1947, which was passed in response to demands from the United States for information required in an investigation of the pulp and paper industry. The most recent legislation is also Canadian. In December of 1984, the Canadian Parliament passed the "Foreign Extraterritorial Measures Act."[42] It contains provisions that would authorize, under certain circumstances, the Attorney General of Canada to prohibit the production of information to foreign tribunals, prohibit compliance with foreign measures, prevent the recognition or enforcement of foreign antitrust judgments, and allow recovery in Canada of damages paid abroad pursuant to foreign antitrust judgments.

Perhaps Canada is more sensitive to the ET problem than many

---

[40] Robinson, *Sovereignty and Data: Some Perspectives* in THE INFORMATION ECONOMY: ITS IMPLICATIONS FOR CANADA'S INDUSTRIAL STRATEGY, PROCEEDINGS OF A CONFERENCE HELD AT ERINDALE COLLEGE, UNIVERSITY OF TORONTO 330 (C.C. Gotlieb Ed., 1984).

[41] *See* Fried, *supra* note 37, at 2.

[42] The Foreign Extraterritorial Measures Act, 49 Can. Stat. 1948.

other countries because of its relatively high degree of dependence on foreign trade and investment, as well as the high level of foreign ownership of Canadian industry. Canada's Ambassador to the United States, Allan Gotlieb, has suggested that: "the issue is qualitatively different in its impact on Canada than in its impact on other countries because of the degree of integration of our respective economies and the extent of U.S. investment in Canada and Canadian investment in the United States."[43] He went on to emphasize the fundamental importance of the issue in the following terms:

> The acceptability of foreign investment depends on the behaviour of the foreign-controlled corporation. A subsidiary of a U.S. corporation operating in Canada will normally find that self-interest dictates that it respond to the same market signals that a Canadian-controlled corporation confronts. However, when the U.S. seeks to influence corporate decision-making abroad it seeks to alter that reaction. In doing so it encourages counter-regulation. And it encourages policies in favour of limiting foreign ownership. Indeed, one of the best arguments against affording national treatment to foreign-controlled corporations is that they respond to the signals of foreign governments.[44]

There appears to be a contradiction in, on the one hand, espousing the concept of "national treatment" for subsidiaries established in a foreign country and, on the other, expecting them to also abide by home-country laws and requirements, even when these are in conflict with the requirements of the host-country. Some meaningful attention to this contradiction will be necessary if friction and frustration in this area are to be reduced.

One of the fundamental functions of international law is to regulate and delimit the jurisdiction of states—of course, in a mutually agreed manner. International law, therefore, cannot provide easy or authoritative answers to the sensitive and sometimes complex jurisdictional questions which arise when a state unilaterally seeks to regulate international transactions. Within the past two decades, the fields of maritime transport, restrictive business practices, and trade sanctions have highlighted such jurisdictional problems. If states seek to protect perceived national and sovereign interests through control and regulation of the uses of data and information, as well as their transfer across national borders, it is not inconceivable that the next two decades will see equally sensitive and complex legal questions arise in the field of transborder data flow. A basic question here is: how can national laws promote national objec-

---

[43] A. Gotlieb, *Conflicting Assertions of National Jurisdiction Over Multinational Enterprises*, (presentation to the Canadian Council on International Law 3) (Oct. 1983). *See also*, Gibbs, *Continuing the International Debate on Services*, 19:3 J. WORLD TRADE L. 199, 214 (1985) which states, "The disequilibrium in the proposals to date for negotiation of rules governing services is that they would seek to impose obligations on host countries with respect to their treatment of TNCs without compatable disciplines being accepted by the home countries or the TNCs themselves."

[44] *See* Gotlieb, *supra* note 43, at 4.

tives and still avoid the effect of controlling or regulating electronic transactions within the borders of other states? Corporations which process, store, transmit or use data in international business transactions will increasingly be subject to different and perhaps contradictory national laws. As transborder data flows increase—as they undoubtedly will—users will increasingly run the risk of being in breach of a national law.

Earlier in this paper, I have given two examples of the extraterritoriality problem: Dresser (France) and the Bank of Nova Scotia. Whether, as suggested above, "rules of the road" for access to and protection of data will adequately deal with these problems, or whether some formalised process of prenotification is also necessary, or additional measures are required, are questions which must be be addressed.

COPYRIGHT

A number of countries are reviewing their legislation on copyright, and it seems appropriate that those national reviews take into consideration the international copyright context, if future problems with TBDF are to be avoided. I will highlight two questions here, one which appears to have achieved a certain degree of consensus and the other which requires a good deal more consideration and discussion. The first relates to protection of computer programs, the second to displays on a screen.

I have already stressed that the main thesis of this paper is that users of TBDF are operating virtually simultaneously under two or more different legal and jurisdictional regimes. It is equally true that the providers of services or the producers of particular products have to rely virtually simultaneously on different legal regimes for the protection of their rights.

Canada is one of those countries reviewing its copyright legislation. A paper entitled "From Gutenberg to Telidon"[45] outlining recommended changes to Canadian Copyright Law was tabled in the House of Commons in May 1984. That report suggested a controversially short five year term protection for computer software.[46] That suggestion was subsequently rejected and the current suggestion is life of the author plus 50 years,[47] which is in accord with the general view in the United States.

While this may be a reasonable resolution of the immediate problem, I would like to draw attention to a recent report prepared by Anne Branscomb for the U.S. Office of Technology Assessment.[48] This report provides a thought-provoking and insightful overview of the implications

---

[45] *From Gutenberg to Telidon, Proposals for the Revision of the Canadian Copyright Act*, SUPPLY AND SERVICES CANADA (Ottawa 1984)[hereinafter *From Gutenberg to Telidon*].

[46] *See id.* at 83.

[47] A CHARTER OF RIGHTS FOR CREATORS 46, (report by the Parliamentary Sub-Commitee on Revision of Copyright) (Oct. 1985) [hereinafter CHARTER].

[48] Branscomb, *The Accomodation of Intellectual Property Law to the Introduction of New Technologies* (a report prepared for the U.S. Office of Technology Assessment) (1985).

of new technological developments for intellectual property law. In it, Branscomb suggests that none of the existing legal systems—patent laws, copyright legislation, and trade secrets—provide a perfect fit for software protection.[49] She goes on to assert that: "The requirement for disclosure in both copyright and patent law benefits neither the creators nor the users of computer software. . . ."[50]

"Thus the requirement of disclosure serves the interests primarily of computer professionals who seek to imitate or modify the system, and, legislatively approved non-disclosure for a limited period may provide a workable arrangement . . . . Such period should be no less than five and no more than ten years."[51] The "non-disclosure period" need not be equated to the "protection period," and might well be a useful concept to adopt, perhaps in conjunction with a review of other aspects of the copyright provisions.

One further point on copyright protection of computer programs is the recommendation by the Parliamentary Sub-Committee on Revision of Copyright that: "The Government should study the possibility of providing an exception to permit the reproduction of a substantial part of a pre-existing program as a non-substantial part of another program."[52]

The Canadian Government's response to this suggested exception has been negative.[53] I raise this point here, not because I favor such exception, but to point out that while some degree of consensus on copyright protection for software has been achieved, other suggestions, as well as the Branscomb proposal, are likely to surface and require attention over the coming months.

The second aspect of copyright that I wish to raise in this paper is that of protection of a display on a screen. The Government's report "From Gutenberg to Telidon" proposed that any tangible copy of a protected work stored in a computer would be protected, but that a copy displayed on a screen would not be protected.[54] This was further supported by the Parliamentary Sub-Committee, but has been put on hold in the Government's response and will be studied further.[55]

No international consensus has yet been achieved on this point. A joint UNESCO-WIPO report in 1982 made the following recommendation:

> In order to harmonize the approach of states in settling the problems relating to input and output and to provide the authors with the real

---

[49] *See id.* at 54.

[50] *See id.* at 88.

[51] *See id.* at 89.

[52] *See* CHARTER, *supra* note 47, at 46.

[53] Canadian Government response to recommendations of The Parliamentary Sub-Committee on Revision of Copyright at 9 (Feb. 1986) [hereinafter *Response to Sub-Committee on Revision of Copyright*].

[54] *See From Gutenberg to Telidon, supra* note 45, at 11.

[55] *See, Response to the Sub-Committee on Revision of Copyright, supra* note 53, at 9.

> possibility of exercising control when their works are put into computer systems, states should consider the desirability to express recognition under their national laws of the exclusive right of the author to make his work available to the public by means of computer systems from which a perceivable version of the work may be obtained. Such a right may apply to the acts of input or output or to the act of input only, the latter being, in this case, the starting-point of control exercised by the author over the destination of his work.[56]

It was obviously easier to reach agreement on the input of a protected work into a computer system, and it was concluded that such an act constituted reproduction within the meaning of copyright legislation. With regard to output, however, the question becomes more contentious, and the report avoids the issue. The main difficulties arise concerning output on a screen. Some argue, as in the Canadian Paper, that as this is not a copy in tangible form it is not protected by copyright. Others argue that it is analogous to a performance or to the showing of a videotape and should therefore receive copyright protection. The question is whether there is a real analogy between performance and broadcasting, on the one hand, and screen display and network distribution, on the other. The French Copyright Act of 11 March 1957, Section 27, seems to deal with this question in the following way:

> Performance consists in the direct communication of the work to the public via, among other things:
> — Public recital;
> — Lyric or dramatic performance;
> — Broadcasting ("diffusion") of words . . . by any process whatsoever;
> — . . . .

It is questionable, however, whether in 1957 the broadcasting of words for display on a screen was contemplated by the drafters of the legislation.

While these difficulties regarding protection of display on a screen remain, there is, as I have indicated, general agreement that protected works stored in a computer should be protected. However, legislation in many countries is not clear on what types of data bases may or may not be protected. There are no general guiding principles for settling this point, and it was not addressed by the joint UNESCO-WIPO committees.

Finally, on the copyright question, I would like to point out that both Bing and Kirby[57] suggest that the new information technologies have "liberated" data and information from the physical media on which they can be represented. Kirby, for example, states that:

> Traditionally, intellectual property law developed around protections

[56] U.N.E.S.C.O., WORLD INT'L PROPERTY ORGANIZATION, C.E.G.O., II, 7 (Aug. 13, 1982).
[57] *See Bing, supra* note 3, at 70; *See Kirby, supra* note 4, at 38.

> 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. 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 made information a commodity.

The points which I raise here suggest that, as an interim measure, copyright or perhaps some modified version of copyright, may be sufficient to deal with immediate and pressing demands. But if some modified version of copyright is necessary, it is not entirely clear what modifications are necessary. For the longer term, little thought is being given to possible requirements.

DATA AS PROPERTY

One of the longer-term requirements which should be given some consideration is the extent to which data and information, as they have been "liberated" from the medium on which they occur, can be regarded as some sort of "property." A Canadian response[58] to an OECD questionnaire on computer-related crime made the following comment:

> "Property" is a very difficult and technical term to attempt to describe. "Property" can loosely be described as something which one has the exclusive right, as against the rest of the world at large, to possess, to do with or to do as one wills, and to prevent all other persons from doing anything in relation to that thing which they are not specifically authorized to do.

This connotation of exclusivity presents difficulty in defining data or information as "property," for it is clear that a person can be in possession of certain data or information which is also known to other people, without in any way depriving them of those data or information. There has indeed been a reluctance, in law, to regard ideas, knowledge, information or data as "property" in any strict sense of the word.

The subsequent OECD report on computer-related crime[59] summarizes the traditional view in the following way:

> Accordingly, information, knowledge, and ideas have not been recognized as constituting "property" for the purposes of the criminal law. Even the civil law has been reluctant to grant a general property status to information, knowledge or ideas, preferring instead to merely clothe particular types of information, knowledge or ideas with some of the

---

[58] Canadian response to OECD questionnaire on computer-related crime, 10.

[59] *See Directorate, supra* note 13, at 21. This is a direct quote from the Canadian Submission.

> attributes of a general property status. For example, statutes such as the Copyright Act and the Patent Act can, if certain conditions are met, grant exclusive rights to an individual to use particular types or forms of representations of information, knowledge or ideas, but even these Acts do not transform that which is patented or copyrighted into a form of traditional property.

In spite of this long tradition in the way in which data, information, knowledge or ideas have been treated, recent events suggest that major changes in concept are beginning to occur. For example, many of the individual states in the United States of America have passed laws in which "property" is defined in the following (or very similar) words: Property includes, but is not limited to, financial instruments, information including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.[60] Many of these state laws appear to copy the wording of previous changes in the laws of other states, and it is not clear to what extent studies were undertaken to consider the implications of these changes in the definition of "property."

Case law in Canada also appears to have taken a turn in this direction. In a case in Ontario, *Regina vs. Stewart*, an individual wished to obtain the names, addresses and telephone numbers of the employees of an hotel, which were protected by the hotel's security system. He approached a security worker at the hotel and offered to pay for the protected confidential data. He was charged *inter alia*, with counselling theft of "information, the property of the . . . Hotel and its employees."

In the "first round," the accused was acquitted. The Court held that information was not "property" as defined in the Canadian criminal law relating to theft. However, in the "second round," the Ontario Court of Appeal, in a majority decision, held that the accused was guilty of counselling theft.[61] In reaching this conclusion, one of the justices stated:

> While clearly not all information is property, I see no reason why confidential information that has been gathered through the expenditure of time, effort and money by a commercial enterprise for the purpose of its business should not be regarded as property . . . if a thing is "property" for the purposes of the civil law, I believe that it is also "property" for the purposes of the Criminal Code.[62]

The appeal to the Supreme Court of Canada is still pending.

It is interesting to note that the dissenting judge in the Ontario Court of Appeal decision believed that:

> It is for Parliament to broaden the criminal definition of the property concept if the needs of modern Canadian Society require it . . . the

---

[60] *See Directorate, supra* note 13, at 23.

[61] 42 Ont. 2d 225 (1983).

[62] *See id.* at 236.

> word "anything" used in § 283 (of the Criminal Code) must be defined and qualified within the context of property and . . . confidential information does not properly fit within that context.[63]

In considering a Bill to extend the Criminal Code definition of "property" to expressly include computer data and software, Parliamentarians, after listening to a series of witnesses brought before a Parliamentary Sub-Committee, stated:

> Some witnesses argued that the definition of the term "property" should be extended to cover "information" or "computer-stored information" so that the existing provisions of the Criminal Code could apply. The sub-committee questions this approach. In our view, it would be ill-advised to grant a proprietary interest in information per se, something which does not exist even in the civil law. For reasons of public policy, the exclusive ownership of information, which, of necessity, would flow from the concept of "property," is not favoured in our socio-legal system. Information is regarded as too valuable a public commodity to have its ownership vest exclusively in any particular individual.[64]

If Canada and the United States are to take divergent approaches to this question of whether data should be regarded as property or not, it is likely to lead to future difficulties. For example, what are the implications for trade with such a difference in attitude towards data and information?

OTHER LEGAL ISSUES

One of the other legal questions that has intrigued me is the utility of trying to distinguish between data and information. In this paper, I have used the two to mean virtually the same thing, yet I am convinced that there is a difference.[65] A supplement to the Oxford English Dictionary, in its definition of "information", acknowledges a contrast with "data": "In administrative data processing, a distinction is sometimes made between data and information by calling raw facts in great quantity 'data,' and using the word 'information' for highly concentrated and improved data derived from the raw facts."[66] Lewis Branscomb has even suggested that: People rarely distinguish between data, information, knowledge, and wisdom. Yet they are as different from one another—and as interlocking—as starch molecules, flour, bread and the flavorful memory of a superb morning croissant.[67]

---

63 *See id.* at 235.

64 REPORT OF THE PARLIAMENTARY STANDING COMMITTEE ON JUSTICE AND LEGAL AFFAIRS 9 (June 1983).

65 *Canadian Perspective, supra* note 6.

66 2 OXFORD ENGLISH DICTIONARY (Oxford V. Press, 1976), citing O.DOPPING, COMPUTERS AND DATA PROCESSING (1970).

67 Branscomb, *Information: The Ultimate Frontier*, 203 SCIENCE 143 (Jan. 1979).

Burk[68] has suggested that there are two views of "data": one based on structure and one based on content. The first defines data as "the smallest indivisible units of information utilized or produced in a specific context." The second defines data as "the raw facts from which information is derived." In either case, he suggests that what constitutes "data" is a function of the context.

A distinction has also been made between "primary data," "processed data" and "analyzed information" in the context of remote sensing by satellite by the Legal, Scientific and Technical Sub-Committees of the United Nations Committee on the Peaceful Uses of Outer Space.[69]

I tend to think of information as something which I can use to make a decision, i.e., as something that is utilizable without further modification. If this is true, information (i.e., what is usable) in one situation, may merely be data in another. For example, shipping documents are information to the shipping clerk, yet those same documents are merely data to the manager, who may need to have them collated and summarized in order to make his ordering decision.

A recent paper[70] appears to build upon a number of these ideas, and stresses the legal importance of making the distinction. For example: "Information is not a thing, but a process or relationship that occurs between a person's mind and some sort of stimulus. On the other hand, data is merely a representation of information or of some concept."

The author goes on to point out that "the new offences in the Canadian Criminal Code are not in relation to information, but data!" There appears to be a need to pay more than academic attention to this distinction.

Another intriguing question may be the distinction between docu-

---

[68] Burk, *The Link Between Data and Documentation*, in GEOSCIENCE INFORMATION: A STATE OF THE ART REVIEW 217 (A. Harvey and J. Diment eds. 1979). He states that the essence of "the concept of 'data' arises from the organization or structure of information, rather than from any intrinsic quality. 'Data' may be defined as the smallest indivisible units of information utilized or produced in the context of a specific intellectual activity. What is or is not 'data' depends on the context in which this information is used or produced . . . . Thus, without specific context and purpose, it is not possible in principle to identify 'data'." *See also*, F. HOSTON, THE INFORMATION MANAGEMENT WORKBOOK (1981).

[69] *Report of the Committee on the Peaceful Uses of Outer Space*, 40 U.N. Supp (No. 20) at 29, U.N. Doc. A-40-20 (1985) defines the following terms:

— primary data; raw data that are acquired by sensors borne by a space object and that are transmitted or delivered to the ground from space by telemetry in the form of electromagnetic signals, by photographic film magnetic tape or any other means:

— processed data; products resulting from the processing of the primary data, needed in order to make such data usable.

— analysed information; information resulting from the interpretation of processed data inputs of data and knowledge from other resources.

Full agreement has not yet been achieved on those definitions.

[70] Piragoff, *Combatting Computer Crime with Criminal Laws*, prepared for *Criminal Law in the Information Society*, Netherlands, Dept. of Justice and Vrije Universiteit (Apr. 1986).

mentary research and propaganda. A film made by the National Film Board of Canada—which has won a number of Oscars for other films it has made—was classified as foreign propaganda in the United States. In Canada it is regarded as a documentary film on acid rain.

Other legal issues raise questions about the law of evidence, and what constitutes the "original" of a document stored in a computer, or perhaps generated by a computer.

I raise these points to emphasize that this paper has not attempted to provide a comprehensive list of the legal issues raised by TBDF. Indeed, as I said at the start, I am not sure how to define what a "legal issue" is and, under these circumstances, it would be foolish to attempt to be comprehensive! This paper is an attempt to merely identify some of the issues which appear worthy of some further thought and, in most cases, some resolution.

CONCLUSION

There is no immediate major crisis, but there have been sufficient irritations in recent years to warrant more consistent attention to legal issues raised by transborder data flow. This requirement may be satisfied by open discussion in a consensus-building forum as governments struggle to understand the implications of developments in information technology. This approach is preferable to confrontation in a negotiating forum, after conflicting approaches have been separately developed at the different national levels.

At this stage no major expensive effort is necessary. This may be the very reason why *nothing* is accomplished. If it is left in abeyance, however, and more and more legislation is developed in different countries to meet perceived needs within the different national contexts, frustrations, conflicts and confrontations will also increase.