NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW

Volume 7 | Number 1 Article 3

Winter 1982

# National Regulation of Transborder Data Flows

Mark B. Feldman

David R. Garcia

# National Regulation of Transborder Data Flows

by Mark B. Feldman* and David R. Garcia**

## I. Introduction

Man's rapidly developing ability to transfer information across national boundaries has become a crucial component in our increasingly integrated world economy. The advent of the computer has revolutionized man's capacity to process and store information. Simultaneously, man's capacity to transmit information has been dramatically increased by a variety of telecommunications innovations, including increasingly effective cable transmissions and orbiting satellites. Together, these two technologies have resulted in a transborder data flow (TDF) essential to expanding international economic development.[1]

The economic implications of TDF are particularly significant for a post-industrial society such as the United States. Many of America's most successful multinational corporations are involved in computer technology, data processing, telecommunications, or information intensive service industries, such as banking and insurance.[2] Advances in TDF technology have had a significant impact on the way companies involved in these and other industries transact international business. For example, it is now possible for a multinational corporation to be monitored on a global scale with a precision undreamed of a decade ago.

Providing data processing services abroad has itself become a multibillion dollar international industry.[3] The export of information processing services and technology is now the single most profitable com-

* Counsel to Donovan, Leisure, Newton & Irvine, Washington, D.C.; Formerly Deputy Legal Adviser of the Department of State; A.B. 1957, Wesleyan University; LL.B. 1960, Harvard University.

** Associate, Donovan, Leisure, Newton & Irvine, Washington, D.C.; A.B. 1976, Harvard University; J.D. 1979, Georgetown University.

1 For purposes of this article the authors define TDF as the transmission from one nation to another of units of information coded electronically for processing or storage by one or more digital computers. This definition purposefully excludes transborder data flows resulting from media products, news broadcasts, voice-to-voice telephone calls, television programming, cablegrams, and telex services.

2 See, e.g., U.S. Dep't of Commerce, The Information Economy: Definition and Measurement, O.T. Pub. No. 77-12(1) (1977) [hereinafter cited as The Information Economy].

3 See International Communications Reorganization Act of 1981: Hearings on H.R. 1957 Before the Subcomm. of the House Comm. on Government Operations, 97th Cong., 1st Sess. 212 (1981) (statement of Richard L. Crandall) [hereinafter cited as I.C. Reorganization Hearings].

ponent of U.S. foreign trade.[4] Advances in telecommunications and computer technologies now enable American computer service companies to offer data processing services world-wide, using data storage and processing facilities maintained in the United States and selected foreign locations.

During the last few years, however, a number of both industrialized and developing countries have begun to regulate and control TDF. This regulation results from a variety of concerns among foreign governments relating to economic independence, cultural identity, and individual privacy rights. The primary motivation for such regulation, however, appears to be the desire to participate in industries that may form the foundation of tomorrow's economy.[5] Although most governments are still formulating their TDF policies, a number of them have taken actions that restrict TDF. Such actions raise serious concerns about future conduct, which could prevent optimal utilization of the new technologies now becoming available to mankind.

At the international level, a number of organizations are now grappling with the TDF issues. The Council of Europe and the Organization for Economic Cooperation and Development have recently issued, respectively, a treaty[6] and voluntary guidelines[7] dealing with the flow of information across national borders. In the United Nations, TDF issues are now on the agenda of the Economic and Social Council and the Commission on Transnational Corporations.[8] The Commission of the European Economic Community (EEC) is actively monitoring developments in the field of TDF, and the European Parliament has passed a resolution asking the EEC Council and Commission to adopt a directive creating a community wide policy.[9] The International Telecommunications Union and, more especially, its Consultative Committee on International Telephone and Telegraph (CCITT), have been involved in overseeing the technical and operational aspects of transnational communication for a number of years. A group of Third World and European countries have formed the Intergovernmental Bureau for Informatics (IBI) to study TDF along with a number of other trade ori-

---

[4] The Information Economy, supra note 2, at 52-55.

[5] An excellent overview of the various policy goals which prompt TDF regulation is provided in Novotny, Transborder Data Flows and International Law: A Framework for Policy-Oriented Inquiry, 16 Stan. J. Int'l Stud. 141 (1980).

[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature January 28, 1981, Europ. T.S. 108. The Convention was signed by representatives of Austria, Denmark, France, the Federal Republic of Germany, Luxembourg, Sweden, and Turkey on January 28, 1981, but as of this date no members of the Council of Europe have ratified the treaty.

[7] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. No. ISBN 92-64-12155-2 (March 1980).

[8] United Nations Economic and Social Council, Report of the Secretariat, Strengthening the Negotiating Capacity of Developing Countries, Transnational Corporations and Transborder Data Flows: An Overview, U.N. Doc. E/C.10/87 (1981) [hereinafter cited as Report].

[9] See Hondius, Data Law in Europe, 16 Stan. J. Int'l Stud. 87, 109 (1980).

ented issues.[10]

In the United States, TDF issues have been addressed by a number of government agencies. These agencies include the Departments of State and Commerce, the Office of the Special Trade Representative, and the Federal Communications Commission.

In addition, a plethora of private organizations have become involved in TDF issues. These organizations include the International Chamber of Commerce (ICC), the Computer and Business Equipment Manufacturers Association, the International Commerce Association, the Information Industries Association, the International Federation of Information Processing Societies, the Association of Data Processing Service Organizations, and the American Bar Association.

Literature about TDF and related issues, written from legal, political, and technical perspectives is growing.[11] Nevertheless, there is still considerable uncertainty as to the nature of the TDF problem and its dimensions. The authors of this article will examine a number of specific examples of TDF regulation by national governments, potentially or actually impinging on the ability of business enterprises to transfer information across national borders. These examples will illustrate the different regulatory strategies being pursued by governments and will perhaps serve to better define the collection of issues that is loosely referred to as "transborder data flow."

## II. Control of Transborder Data Transmission: Japan and Germany

Transborder data flow is equally dependent upon communications and data processing technology. Therefore, the most sophisticated computer located in Country A cannot participate in a TDF exchange without some mechanism for transporting data from other countries into Country A for processing and/or storage and then back out again. Such critical communication links are particularly vulnerable to national regulation.

For example, two American computer companies, Control Data Corporation (Control Data) and Tymshare Inc. (Tymshare), decided several years ago to offer a broad range of data processing services to clients in Japan, utilizing computer main frames located in the United States. For almost five years, however, both companies were unable to offer the types of services originally planned because of regulatory difficulties encountered in attempting to set up telecommunications links for transmitting data back to the United States.

---

[10] IBI is an international organization composed of approximately 30 member countries. IBI's members are primarily developing countries, although Italy, France, and Spain are also members. See UNESCO, Informatics: A vital factor in development 19 (1980).

[11] For some flavor of the wide variety of perspectives reflected in the literature of TDF, as well as the rapidly increasing extent of that literature, see Novotny, Transborder Data Flows: A Bibliography, 16 Stan. J. Int'l Stud. 181 (1980).

At the present time, the most likely mechanism for such transmission would be a "dedicated" or private leased telephone line between Japan and the United States. The actual hookup could be accomplished with either a transoceanic cable or a communications satellite. Such an arrangement would involve leasing the telephone line at a fixed monthly rate with guaranteed continuous access to the circuit. In Japan such a line must be leased from Japan's international record carrier, Kokusai Denshin Denwa Co., Ltd. (KDD).

While both Control Data and Tymshare have obtained leased lines from KDD, the lease agreements until recently contained restrictions that severely impeded the capacity of the companies to provide services and compete effectively in Japan.[12] For example, under these agreements both companies were prohibited from connecting the leased line to more than one computer center within the United States.[13] Thus, although Control Data has five different data processing locations in the United States, each performing distinct types of processing operations, Control Data could offer Japanese customers direct access to the services and computer capabilities available at only one of its American locations. Moreover, the application procedure required to obtain a dedicated line from KDD involves an extremely detailed inspection of the applicant's hardware and software. The thoroughness of this inspection has led Tymshare to suspect that KDD might be using the application procedure to acquire technology rather than to monitor the operations of a foreign company.[14]

Both companies have also voiced concern that they might not be able to continue leasing private transatlantic lines when KDD begins using its new usage sensitive data network known as "VENUS."[15] Tymshare has stated that it was offered an arrangement whereby it would be allowed to offer its entire range of computing services in Japan, but would be required to utilize a usage sensitive line. The cost of usage sensitive service depends upon how often it is used and how much information is transmitted. According to Tymshare, the usage sensitive pro-

---

[12] See International Data Flow: Hearings Before a Subcomm. of the House Comm. on Government Operations, 96th Cong., 2d Sess. 21-22 (1980) (statement of Philip C. Onstad, Manager of Telecommunications Policy, Control Data Corp.). See also id. at 63 (statement of Warren E. Burton, Vice President, Tymshare, Inc.) [hereinafter cited as Data Flow Hearings].

[13] Id. at 22. The contract between Control Data and KDD provided that the leased line into the U.S. could only hook up to one processing center, although five such centers are available. KDD took the position that the transfer of data from one U.S. center to another would constitute message-switching, which is prohibited by Japanese law. Id. In other words, KDD felt that if messages could be transmitted between two or more points within the U.S., then the two computer companies would in effect have gone into the communications business and could, at least potentially, create their own telephone switching network. See W. Union Int'l, Inc. (File No. I-T-C 2678-1); ITT World Commun., Inc. (File No. I-T-C 2664-11); and RCA Global Commun., Inc. (File No. I-T-C 2667-8), petition to deny before F.C.C. (filed April 11, 1979, by Control Data) [hereinafter cited as W. Union Int'l, Inc.].

[14] Data Flow Hearings, supra note 12, at 63. In this regard, it is interesting to note that KDD's sister agency is the largest supplier of computer services in Japan. Id.

[15] Id. at 22.

posal offered by KDD would increase the price of Tymshare's computing services in Japan by ten times over that of present levels, rendering Tymshare virtually incapable of competing effectively in the Japanese domestic computer service market.[16]

In addition to illustrating the impact of government regulation on transborder data transmission, the experiences of Tymshare and Control Data also reveal the extent to which responsibility or authority to deal with TDF controls is spread over a large number of U.S. government agencies. Because KDD is an instrument of the Japanese Government, Tymshare and Control Data looked first to the United States government for assistance.[17] Both companies contacted numerous government agencies, including the Japan-United States Trade Facilitation Committee in the Department of Commerce, the National Telecommunications & Information Administration of the Department of Commerce, the Office of the Special Representative for Trade Negotiations, and the State Department.[18]

Under the terms of section 214 of the Communications Act of 1934,[19] the interested U.S. international record carriers had to receive authorization from the Federal Communications Commission (FCC) in order to commence the usage sensitive VENUS service between Japan and the United States. Control Data opposed that application, arguing that if the application were granted KDD would discontinue leased line service and would force all computer service companies operating from the United States to utilize the usage sensitive VENUS service.[20] The application was also opposed by the Computer and Business Equipment Manufacturers Association (CBEMA) and the Association of Data Processing Service Organizations (ADAPSO). Both CBEMA and ADAPSO argued in submissions to the Common Carrier Bureau of the FCC that approval should be conditioned on the continued availability of flat rate leased lines between Japan and the United States.[21]

The international record carriers responded by emphasizing that the usage sensitive service being applied for was designed to serve small and medium volume users who did not have the resources to offer data processing on the scale of Control Data or Tymshare.[22] They pointed out that similar services, commenced between the United Kingdom and

---

[16] Id. at 63.

[17] Id. Because Post, Telephone, and Telegraph administrations (PTTs) are virtually always government owned and operated (the U.S. being a major exception), this situation will exist in almost every negotiation between an American enterprise and a foreign PTT. See Fishman, Introduction to Transborder Data Flows, 16 Stan. J. Int'l Stud. 1, 14 (1980).

[18] Data Flow Hearings, supra note 12, at 22-23, 63.

[19] 47 U.S.C. § 241 (1976).

[20] Data Flow Hearings, supra note 12, at 23. See also memorandum opinion cited note 22 infra.

[21] See W. Union Int'l, Inc., note 13 supra, Comments to F.C.C. (filed April 11, 1979, by CBEMA), and Application for Review (filed Jan. 14, 1980, by ADAPSO).

[22] See W. Union Int'l, Inc., note 13 supra, Memorandum Opinion of F.C.C. at 4 (adopted Dec. 11, 1979).

the United States almost three years before, had not resulted in the curtailment of the availability of private leased line services between the United States and the United Kingdom.[23] The applicants also provided documents from KDD in which the Japanese agency promised to continue leased line services.[24] In addition, the applicants suggested that the FCC's review of KDD policies might well interfere with Japanese sovereignty.[25]

On December 11, 1979, the Common Carrier Bureau of the FCC ordered commencement of the VENUS service for a one year experimental period.[26] The Common Carrier Bureau observed that the new service would suit the needs of a variety of small- and medium-sized computer service companies. In addition, the Common Carrier Bureau noted that private line service had never been discontinued or restricted in a case in which usage sensitive services had been authorized. The Bureau also stated that "no persuasive evidence has been submitted to indicate that a discontinuance of private line service to Japan will occur" if the VENUS service were authorized.[27] Finally, the Bureau noted that the CCITT resolutions, invoked by those opposing the applications, were not legally binding and that in any case no Telegraph Regulations had been violated.[28]

The authorization for the VENUS service was continued by six month extensions issued on December 15, 1980, April 20, 1981, and August 14, 1981.[29] On October 15, 1981, a further one year extension to October 16, 1982, was granted by the Common Carrier Bureau. The Bureau stated that because "delicate bilateral negotiations regarding the availability of private line services [were] taking place" a further extension was warranted.[30] The VENUS service, therefore, continues at this time on a temporary basis. The Common Carrier Bureau has not acted on applications for permanent authority and the full Federal Communications Commission has not yet considered the matter.[31]

---

23 Id.

24 Id.

25 Id.

26 Id. at 7.

27 Id. at 6.

28 Id. at 6-7.

29 W. Union Int'l, Inc., note 13 supra, Order and Authorization by F.C.C. at 2.

30 Id.

31 The VENUS application was not the first instance in which an application for regulatory approval was resisted by parties seeking to gain leverage over a foreign PTT. In September, 1979, three U.S. telecommunications companies petitioned the FCC for authorization to begin usage sensitive data service between the United States and Hong Kong. The application was resisted by ADAPSO acting at the request of General Electric Company, which had been denied access to a private leased line by Hong Kong's PTT, Cable and Wireless, Ltd. The FCC refused to link the U.S. common carrier applications with the denial of leased line service to General Electric, stating that "it could not force foreign correspondents to provide matching halves of particular circuits, or services which we would require the U.S. carriers to provide now, or in the future." ITT World Communications, Inc., Western Union International Line, Inc., RCA Global Communications, Inc., F.C.C. File Nos. I-T-C2664-2, I-T-C2658-2, I-T-

The authors have been advised that on June 1, 1981, Control Data began to provide computer processing services in Japan utilizing an unrestricted leased line between Japan and the United States. Therefore, almost five years of negotiation were necessary before Control Data could gain access to an unrestricted lease line for the provision of data processing services into Japan. Tymshare is still negotiating with the Japanese over technical points, but now anticipates that an agreement will be reached in the first part of 1982.

The experiences of Tymshare and Control Data in Japan are not isolated incidents.[32] There is also considerable concern about the policies of the German post and telegraph administration, the Bundespost. The Bundespost controls access to the type of dedicated lease line necessary for large-scale data transmission. Since late 1978, the Bundespost had, from time to time, indicated privately to a number of American companies that all leased line services would be eliminated as of January 1, 1982 in favor of an usage sensitive regime.

In recent months, however, the Bundespost has indicated that the new regime would not go into effect until later in the year and that, even then, leased lines would still be available to those companies that maintained significant data computer processing facilities within Germany. The proposed exception for firms utilizing computer facilities within Germany demonstrates that restriction of access to leased lines can be used by the local PTT, not only to increase revenue, but also to encourage the placement of computer facilities within the country regulating access to the leased line. Restriction of access to leased lines could also be used to discourage the offering of computer services by foreign companies in an effort to foster the growth of the domestic data processing and computer industries. Whatever the motivation, a country's requirement that computer facilities be placed within that country as a precondition for the granting of access to dedicated leased lines amounts

---

C2657-3 (released July 12, 1978) (Memorandum Opinion, Order and Authorization) at 11. In comparison, the FCC's decision to proceed by interim extensions of temporary authority in the VENUS case due to admitted awareness of "delicate bilateral negotiations" arguably evidences a willingness to become aware of and react to, broader developments on the international scene as part of in its decision making.

[32] There have also been reports that European PTTs have established a data transmission network which has excluded American companies desiring to provide computer services. The system involved, EURONET, was created by setting aside some portion of each PTT's transmission capability solely for the transmission of data, and combining this capacity with computers at various access points in the countries involved. The resulting system allows a user to access the system and move data without having to purchase his own computers. Instead a user can either buy or lease a terminal in each of the countries served by EURONET and move data in this fashion. Some American companies have reported to STR that EURONET's present policy is to exclude computer service companies not from EEC countries from utilizing the EURONET system. See I.C. Reorganization Hearings, supra note 3, at 137-49 (appendix to statement of Geza Feketekuty, Assistant U.S. Trade Representative for policy development). Even more recently, however, Mr. Feketekuty has been quoted as saying that American companies are now gaining limited access to EURONET. See Seaman, Transborder Data Flow: Diffusing a Burning Issue, 13 Computer Decisions 58, 58 (1981).

to a "performance requirement" of the type that tends to create an artificial distortion in international trade and investment.[33] The particular application may be new, but it is a classic example of the requirement that an enterprise make an investment in-country as a condition of conducting operations there.

In November, 1981 the authors were informed that the German PTT was contemplating measures that would force foreign companies to utilize costly use-sensitive public service lines for data transmissions to and from Germany, irrespective of the maintenance of computer facilities in Germany. Such restrictions on the use of dedicated leased lines could create a significant barrier to the provision of computer services to Germany from locations outside the country. Whether a PTT requires utilization of in-country computer facilities as a condition for access to leased lines or compels the utilization of more expensive facilities such as usage sensitive lines, tremendous pressure is placed on the American enterprise to deploy hardware abroad rather than relying on terminals abroad to transmit data back to computing facilities in the United States for storage or processing. For example, as a result of such pressures both Control Data and Tymshare have decided to establish computer facilities in Japan.[34]

If applied to internal corporate TDF, such restrictions would affect the operations of many multinational enterprises. While some companies may be able to adjust to such a system without undue hardship, other enterprises may not be in position to respond by deploying computer facilities abroad. Not every enterprise has the resources or the inclination to invest in computer facilites in every country in which it conducts business. For example, one large American bank has indicated that if significant restrictions are placed on the availability of leased lines it will not be able to centralize all data processing for its multinational operations, a move intended to cut costs and improve service.[35]

## III. Bilateral Treaties of Friendship, Commerce and Navigation

The issues raised by TDF may cause one to question whether the existing international legal regime is adequate to deal with TDF. In some situations, however, an American enterprise subjected to inequitable or discriminatory practices affecting TDF may enjoy some protection under the legal regimen established by the bilateral Treaties of Friendship, Commerce and Navigation and similar agreements (FCN treaties). The United States has concluded FCN treaties with more than thirty

---

[33] For a study of the worldwide use of incentives and performance requirements see Int'l Trade Administration, U.S. Dep't of Commerce, The Use of Investment Incentives and Performance Requirements by Foreign Governments (1981).

[34] See Data Flow Hearings, supra note 12, at 62-63.

[35] Id. at 113 (statement of Robert E. L. Walker, Vice President and Counsel, Continental Illinois Bank).

foreign states,[36] including the Federal Republic of Germany,[37] France,[38] and Japan.[39]

While individual treaties vary in detail, they generally have the same basic scheme. With regard to TDF, the treaty regime includes (1) national treatment for business enterprises except where specified activities, notably communications, are involved; (2) most-favored-nation treatment where national treatment does not apply; and (3) general guarantees of "fair and equitable" treatment.

For example, Article VII(1) of the FCN Treaty with the Federal Republic of Germany stipulates that "[n]ationals and companies of either Party shall be accorded, within the territories of the other Party, national treatment with respect to engaging in all types of commercial, industrial, and other activity for gain . . . ."[40] National treatment is defined as treatment "no less favorable than the treatment accorded . . . in like situations" to nationals or companies of the host country.[41] Further, under the German Treaty, enterprises controlled by nationals of one party "shall in all that relates to the conduct of the activities thereof, be accorded treatment no less favorable than that accorded like enterprises controlled by nationals or companies of such other Party."[42] Such national treatment need not be accorded aliens "engaged within its territories in communications," provided that new limitations on national treatment are not applied to established activities.[43] This exception does not apply, however, to the use of communications facilities in the conduct of other business activities, such as banking. Further, the German Treaty stipulates that "neither Party shall deny to transportation, communications and banking companies of the other Party the right to maintain branches and agencies, in conformity with the applicable laws and regulations, to perform functions necessary for essentially international operations in which they engage."[44]

Therefore, unless an American company falls within one of the treaty exceptions, it is entitled, as a matter of international law, to carry out its business activities, including data processing and international communications, on the same basis as a German enterprise. In addition, Article XVII(2) of the Treaty obligates each Party to provide nationals

---

[36] See U.S. Dep't of State, Treaties in Force (1981).

[37] Treaty of Friendship, Commerce, and Navigation, Oct. 29, 1954, United States-Germany, 7 U.S.T. 1839, T.I.A.S. 3593.

[38] Convention of Establishment, Protocol, and Declaration, Nov. 25, 1959, United States-France, 11 U.S.T. 2398, T.I.A.S. 4625.

[39] Treaty of Friendship, Commerce, and Navigation, April 2, 1953, United States-Japan, 4 U.S.T. 2063, T.I.A.S. 2863.

[40] Treaty, United States-Germany, supra note 36, art. VII, para. 1.

[41] Id. art. XXV, para. 1.

[42] Id. art. VII, para. 1(c).

[43] Id. art. VII, para. 2. Other exceptions include air or water transport, taking and administering trusts, banking involving deposits, and the exploitation of natural resources. Id.

[44] Id.

of the other Party "fair and equitable treatment"[45] as compared with that accorded to the nationals, companies, and commerce of any third country, with respect to, *inter alia*, "the sale of any service sold by the Government or by any monopoly or agency granted exclusive or special privileges."[46] This same general regime applies in the territories of other U.S. FCN treaty partners.[47]

Generally, any dispute arising under an FCN treaty, which cannot be settled by diplomacy or other agreed means, "shall be submitted to the International Court of Justice."[48] Issues arising under treaties are generally taken up diplomatically between governments, but American courts may enforce treaty rights held to be self-executing upon the application of an interested private party.[49] In addition, U.S. regulatory agencies such as the FCC have also considered treaty rights when relevant to a pending matter.[50] A company injured by administrative action in a foreign country, which it believes violates a treaty in force, may also wish to consider whether comparable relief is available under the laws of that foreign state.

## IV. Regulation of Computer Hardware: Brazil

TDF tensions are not confined to industrialized nations. A consequence of the emerging world economy is the rapid dissemination of data processing and communication technology in the third world. This rapid dissemination is a function of international trade and of the management operations of multinational corporations (MNCs). TDF regulation in developing countries is characterized by a preoccupation with noneconomic factors, such as perceived threats to national security or sovereignty as a result of unrestricted TDF. Of course, developing countries are not without conventional economic motives as well. Indeed, the existence of both economic and political motivations has contributed in Brazil to comparatively extreme types of TDF regulation. Such regulation includes prohibition of certain types of hardware and the outright refusal to allow the import of data processing services in some cases.[51]

---

[45] Id. art. XVII, para. 2.

[46] Id. art. XVII, para. 2(c).

[47] See French Treaty, supra note 38, arts. IV, V; Japanese Treaty, supra note 39, arts. VI, VII. See also OECD Declaration on International Investment and Multinational Enterprises, 15 Int'l Legal Materials 967 (1976) (reproduced from OECD Press Release of June 21, 1976). The Declaration establishes similar principles of national treatment for enterprises owned or controlled by nationals of all member countries operating in their territories. Id. II para. 1. This Declaration incorporates solemn policy commitments of all the OECD member states except Turkey, and a legally binding Decision of the OECD Council provides for notice and consultation respecting exceptions to national treatment. Id. at 979.

[48] Protocol to Treaty, United States-Germany, supra note 37, para. 24.

[49] See, e.g., Spiess v. C. Itoh & Co., 643 F.2d 353 (5th Cir. 1981).

[50] See In re French Telegraph & Cable Co. (File No. I-T-C 2650) Memorandum Opinion & Order (adopted March 30, 1979).

[51] See Trade Barriers to Telecommunications, Data and Information Services, reprinted in I.C. Reorganization Hearings, supra note 3, at 140 (statement of Geza Feketekuty, app. B).

Although among developing countries such regulation is still the exception rather than the rule, a number of Third World countries have expressed an interest in creating such regulation, or are currently drafting such controls.[52]

A flavor of current Third World attitudes towards TDF may be obtained by examining a recent report entitled *Transnational Corporations and Transborder Dataflow: An Overview*, issued by the U.N. Secretariat for the Commission on Transnational Corporations.[53] The Report's avowed purpose was to enhance the negotiating capacity of developing countries in their dealings with multinational corporations.[54] The Report identifies what its authors perceive as potentially negative effects of TDF upon economic and cultural development as well as the threat it poses to national sovereignty.[55] In economic terms, the Report describes TDF as a major economic opportunity, which is now largely the province of MNCs based in developed countries, especially those based in the United States.[56] In noneconomic terms, the Report contends that the processing and storage of data in a foreign location inhibits a country's ability to influence and direct its own political and cultural future.[57]

Brazil is the most arresting example of TDF regulations in the context of a developing country because of the explicit goals of TDF regulations articulated by the Brazilian government and the severe character of the regulations. The policies behind Brazil's program of TDF regulation have been clearly delineated in two recent actions by the Brazilian government. First, in 1979 Brazil created the office of the Special Secretariat of Informatics (SEI) and issued an accompanying Presidential guideline describing Brazil's information policy.[58] The espoused policy to be implemented by the SEI is openly protectionist. The national policy mentions a commitment to protect information to ensure personal privacy. The main thrust of the policy, however, is a commitment to stimulate development of domestic software and hardware capability through the systematic exclusion of potentially competitive foreign goods, the increased direct ownership of computer facilities by the state, and the establishment of technical standards and regulations favorable to domestic products.[59]

Second, in September 1980, the Special Commission for Teleinformatics (Commission), a body created by the SEI to discuss is-

[52] See generally M. Masmoudi, The New World Information Order (1978); United Nations Economic and Social Council, Final Report: Intergovernmental Conference on Strategies and Policies on Informatics, UNESCO, SC/MD/63 (1979).

[53] Report, supra note 8.

[54] Id. at 4.

[55] Id. at 21-23.

[56] Id. at 17.

[57] Id. at 23.

[58] Brazilian Executive Decree No. 84.067 (October 8, 1979).

[59] Brizida, The Brazilian Transborder Data Flow Policy, 4 Transnational Data Report, No. 3 at 19 (1980).

sues arising out of the convergence of telecommunications and data processing technologies, issued a report.[60] In that report the Commission endorsed SEI's practice of requiring prior approval before allowing the establishment of transmission links to data banks outside Brazil, and recommended the continuation of this practice. The Commission also argued for as complete a ban as possible on the importation of all foreign computer products. In addition, the Commission embraced the concept of TDF regulation as a mechanism for controlling the activities of foreign enterprises in Brazil. The Commission suggested that Brazilian policy should be aimed at strengthening Brazilian subsidiaries in relation to foreign parent companies by encouraging the retention of information within Brazil.[61]

Although at first glance Brazilian regulation of TDF links may appear similar to the Japanese authorization procedure, in practice Brazil's authorization procedure goes considerably beyond just controlling access to leased lines. Brazil is also beginning to control what types of hardware may be imported into Brazil and the types of services that may be offered once computing equipment is installed.

Applications for permission to engage in transborder transmissions of data are processed by the Brazilian telephone company, Embratel. TDF links are approved for a maximum of three years and renewal is possible after the three year period upon the filing and approval of another application.[62] Making an application involves completion of the SEI's International Data Link Reporting Form, a lengthy document, which requests disclosure of extensive information. The enterprise must provide a detailed description of its owners and principals and their connections with Brazil.[63] The applicant must also describe any Brazilian entities that would benefit from the service requested.

In addition, the applicant must describe the type of TDF link it plans to employ, including the number of transmission lines contemplated, the degree of use on each line or lines, the type of hardware and software to be used, and the transmission speed of the equipment being utilized.[64] Total expected expenditures for equipment, personnel, royalties, and training in connection with the link in question must also be described in detail.[65] The applicant is required to explain how Brazil will benefit from institution of the applicant's service. Moreover, to the extent that the service relies upon data processing services or equipment in other countries, the applicant must state whether the processing could

---

60 Id. at 23.

61 Id.

62 Id. at 19.

63 International Data Link Form (unofficial translation), 4 Transnational Data Report, No. 3 at 24-25, paras. I.3, I.4 (1980).

64 Id. paras. II.1, II.2, IV.2, IV.3.

65 Id. para. II.2(e).

feasibly be done in Brazil.[66] If the proposed TDF link involves the use of imported computer equipment, the applicant must state whether alternative equipment is available in Brazil and, if so, why such equipment is inadequate.[67]

The applicant must also describe, with particularity, data that it expects to transmit from or receive inside Brazil. This description must include a listing of the files and data bases to be utilized in the link, the exact location of these files and data bases,[68] and the substantive content of the data being transmitted. All parties who are expected to make use of the data must be listed with an estimate of the length of time they will use the data.[69] Finally, the applicant must declare whether information that is stored outside of Brazil can be recovered in the event of any type of litigation in Brazil.[70]

These procedures provide the Brazilian government with the means to control both the TDF equipment and the process of TDF. While most applications have been approved, permission has been denied in two situations. First, applications by Brazilian subsidiaries of foreign MNC's for intracorporate TDF links have been denied. At least one such application has been rejected on the ground that computers available inside Brazil were adequate to perform the services required by the Brazilian subsidiary.[71] Second, applications by computer service companies to provide data processing services in Brazil have also been denied. An official of the SEI has stated that some of these refusals result from the Brazilian government's uncertainty as to the potential social and economic ramifications of the proposed service.[72]

The Brazilian approach to TDF is the antithesis of the open market philosophy, which permitted the expansion of the world economy in the post-war period. For instance, Brazil's announced intention to restrict importation of computer products in an effort to promote the Brazilian computer industry, if actually implemented, seemingly would conflict with provisions of the General Agreement on Tariffs and Trade (GATT), to which Brazil is a signatory.[73] There also appear to be potential difficulties in reconciling restriction of the importation of computer products and services with Brazil's strong emphasis on technology transfer. It is too soon to tell, however, whether this policy will be rigorously applied

[66] Id. para. III.1(c).
[67] Id. para. III.1(d).
[68] Id. para. IV.5.
[69] Id. para. III.2(c).
[70] Id. para. III.2(e).
[71] Brizida, supra note 59, at 19.
[72] Id.
[73] General Agreement on Tariffs and Trade, open for signature Oct. 30, 1947, arts. XI, III paras. 1, 2, 61 Stat. Parts (5) and (6), T.I.A.S. No. 1700, as amended (text of GATT in force in 1979 may be found at 2A Comprehensive Handbook of the United Nations 419-58 (Dr. Min-Chuan Ku ed. 1979)); but cf. id. at art. XVIII, which permits developing countries to establish protective measures for new industries.

and, if so, whether it can be sustained without impairing the modernization of Brazil's economy.[74]

## V. TDF Regulation Through Personal Privacy Laws

A number of foreign countries have enacted laws designed to ensure the privacy and security of electronically stored data.[75] The majority of these laws contain provisions regulating TDF as an adjunct to the more general regulation of the storage and use of data. This relationship between privacy laws and TDF regulation has generated a wide range of important issues.[76] The discussion below focuses on the specific TDF provisions found in privacy laws already in effect in a number of European countries.

Levels of data protection, methods of enforcement, and rights granted data subjects differ from country to country. Consequently, MNC's operating in a number of different countries may be confronted with widely differing, perhaps even contradictory, privacy regulations.[77] In some cases, the regulations have led to a degree of data inspection and expense that businesses find to be excessive even in light of the purpose of the privacy laws. Many business leaders are concerned about the protectionist impact and the possible unstated protectionist motivation, which they suspect may be the real reason for the passage of data privacy protection statutes.[78]

Existing privacy laws exhibit a tremendous diversity with respect to

---

[74] See Transborder Data Flow Committee, A Review of the Economic Implications of Canadian Transborder Data Flows, submitted to the Dep't of Communications of Canada (May 1981). The Committee's position is that TDF restrictions will inhibit economic development.

[75] Laws designed to control the collection of personal data have been passed in France, West Germany, Sweden, Denmark, Luxembourg, Norway, and Austria. See infra notes 89, 84, 93, 81, 129, 99, 82. Such legislation has been proposed in Spain, Great Britain, and Italy. In addition, both Canada and the United States have enacted privacy laws that are applicable only to information collected by the respective governments of those two countries. See infra notes 79, 80.

[76] For instance, a controversy now rages around whether data protection laws should be extended to give substantial rights to legal as well as natural persons. The basic jurisdictional provisions of each of the statutes discussed in this section typically begin by defining what sorts of "data subjects" have rights with respect to data about them being stored by electronic means. At present, the statutes in Austria, Denmark, Luxembourg, and Norway extend substantive rights to both corporations and individuals. In a situation in which a data subject is guaranteed access to data about him, extension of substantive data protection rights to legal persons in theory allows one corporation access to all data concerning it stored within the files of another corporation, including its competitors. See Hogrebe, Guidelines Concerning the Protection of Privacy and Transborder Data Flows of Personal Data, OECD Doc. No. DSTI/ICCP/81.25 (Sept. 1, 1981). For recent discussions of the broad range of political and legal issues generated by privacy legislation in Europe, the authors recommend the following three articles as well as the sources cited within these articles: Hondius, supra note 9; Stadlen, Survey of National Data Protection Legislation, 3 Computer Networks 174 (1979); Evans, European Data Law, 29 AM. J. COMP. L. 571 (1981).

[77] See Rooms & Dexter, Data Protection for Private Multinational Networks, 3 Computer Networks 205-14 (1979).

[78] See Data Flow Hearings, supra note 12.

the degree to which transfers of data across national borders are regulated. At one extreme are the privacy acts in Canada[79] and the United States,[80] which are directed only at information in government possession and are restricted to data about persons residing within each country. At the other extreme are TDF provisions, such as those of Denmark[81] and Austria,[82] which contain detailed provisions concerning the circumstances under which electronically stored data about any person may be transmitted across the border of the country involved.[83]

### *A. The Federal Republic of Germany*

The German Privacy Statute,[84] although otherwise quite detailed, has no provisions directly addressed to TDF. Nevertheless, certain generally applicable provisions are clearly pertinent to transnational data transfers. Data processors are prohibited from disseminating or storing data unless the rights of the data subject, described at length elsewhere in the statute,[85] are protected.[86] Although data processors are subject to reporting requirements,[87] TDF links do not require advance approval, unlike some other privacy statutes discussed below. Private parties may be temporarily restrained, however, from transmitting data pending a determination by the Civilian Regulatory Authority.[88]

### *B. France*

The privacy statutes in France,[89] Sweden, and Norway are more intrusive than the German statute. The French statute provides that pri-

---

[79] Canadian Human Rights Act, ch. 33, [1976-77] Can. Stat. 887 (1977), reprinted in Compilation of Privacy Legislation in OECD Member Countries, OECD Doc. No. DSTI/ICCP/79.11/04 (March 5, 1979) [hereinafter cited as Canadian Privacy Act].

[80] 5 U.S.C. § 552(a) (1976).

[81] Private Registers Etc. Act of 1978, § 21(1), Act. No. 293 (Denmark), approved translation reprinted in Compilation of Privacy Legislation in OECD Member Countries, OECD Doc. No. DSTI/ICCP/79.11/05 (March 5, 1979) [hereinafter cited as Danish Privacy Act].

[82] Federal Act of 18th October, 1978, on the Protection of Personal Data (Data Protection Act), 1978 Bundegesetzblatt No. 565 (Aus.), approved translation reprinted in Compilation of Privacy Legislation in OECD Member Countries, OECD Doc. No. DSTI/ICCP/79.11/02 (March 5, 1979) [hereinafter cited as Austrian Privacy Act].

[83] See Danish Privacy Act, supra note 81, §§ 21(1)-(3); Austrian Privacy Act, supra note 82, §§ 32-34.

[84] Federal Data Protection Act of January 27, 1977, 1977 BGBI I.201 (W. Ger.), approved translation reprinted in Compilation of Privacy Legislation in OECD Member Countries, OECD Doc. No. DSTI/ICCP/79.11/01 (March 7, 1979), also reprinted in U.S. Dep't of Commerce, Selected Foreign National Data Protection Laws and Bills 10-42 (1978) [hereinafter cited as W. German Privacy Act].

[85] Id. § 4.

[86] Id. § 1.

[87] Id. §§ 22-25.

[88] Id. § 13.

[89] Act 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties, [1978] J.O. 227, approved translation reprinted in Compilation of Privacy Legislation in OECD Member Countries 7, OECD Doc. No. DSTI/ICCP/79.11/08 (March 5, 1978), also reprinted in U.S. Dep't of Commerce, Selected Foreign National Data Protection Laws and Bills 48 (1978) [hereinafter cited as French Privacy Act].

vate entities wishing to store and transmit personal information in France must file an undertaking and reporting form with the National Data Processing and Liberties Commission (Data Commission).[90] The report must specify "whether the processing is intended for the dispatch of personal data between France and another country, in any form, including the case where it involves operations carried out partly in France on the basis of operations previously performed outside France."[91] Use of the language "between France and another country" seems to imply that the reporting requirement extends not only to the transfer of data generated in France for processing outside of France but also to the transfer to France of information that has undergone data processing outside of France.

The French statute does not require prior approval before commencement of data storage and transmission. The statute does, however, give the Data Commission the discretionary authority to make particular TDF activities subject to prior approval after the initial notification process.[92] The Data Commission does not have this authority with respect to data processing activities in France that do not involve TDF.

### *C. Sweden*

Enacted in 1973, Sweden's privacy statute was Europe's first such statute.[93] Under the Swedish law the formation of a data bank, which will contain personal information, is subject to prior approval by a Data Inspection Board (DIB).[94] Specific DIB approval must be obtained for transborder exchanges of information.[95] Data transmissions within Sweden are subject to general regulations promulgated by the DIB after initial approval is obtained for creation of a data bank.[96] Therefore, the law subjects transborder data transmissions to more stringent regulation than transmissions of data from one point to another within Sweden. The DIB's authority is activated under the Swedish statute "[i]f there is reason to believe that personal information will be used for [automatic data processing] abroad. . . ."[97] Instances already documented by other authors in which specific firms have been denied TDF approval demonstrate that the Swedish DIB's approval of transborder data transmissions is hardly *pro forma*.[98]

---

[90] Id. § 15.
[91] Id. § 19.
[92] Id. § 24.
[93] Data Act of May 11, 1973 (Sweden), translation reprinted in Compilation of Privacy Legislation in OECD Member Countries, OECD Doc. No. DSTI/ICCP/79.11/18 (March 5, 1979), also reprinted in U.S. Dep't of Commerce, Selected Foreign National Data Protection Laws and Bills 71 (1978) [hereinafter cited as Swedish Privacy Act].
[94] Id. § 2.
[95] Id. § 11.
[96] Id. § 6.
[97] Id. § 11.
[98] See Stadlen, supra note 76, at 185-86.

### D. *Norway*

Under the Norwegian privacy statute international data transmissions must be approved on a case-by-case basis.[99] Although the statute does provide for the promulgation of regulations creating exceptions to this requirement,[100] none has been issued to date. Data processing inside Norway is subject to general prior approval, but there is no domestic counterpart to the case-by-case approval required for transborder transfers of data. The statute further provides for the drafting of regulations to ensure cooperation between the Norwegian data protection agency, the Data Surveillance Service, and administrative authorities in other countries involved in the protection of electronically processed information.[101] This last provision seems to be designed for the day when Norway will take steps to harmonize its data protection laws with those of other European countries, either as a member of the EEC or pursuant to the Council of Europe's Treaty on Personal Privacy Protection.[102]

### E. *Denmark*

The privacy statutes of Austria and Denmark are more complex and more specific than any of the other European statutes regulating TDF. Both statutes prescribe substantive principles for the protection of personal information and require prior authorization or licensing of TDF by a national data control authority.[103]

Under the Danish law, data may not be gathered in Denmark or transmitted out of Denmark without a license. The law thus requires prior approval by the Data Surveillance Authority (DSA) before personal data may even be gathered for potential transfer outside the country.[104] Further, the Danish act prohibits the gathering of certain types of data under any circumstances.[105] The statute explicitly extends this prohibition to the gathering of data to be stored outside of Denmark.[106]

The DSA must also review proposed TDF links to ensure that the contemplated transfer of data will not significantly lower the level of protection accorded to data in Denmark.[107] If, however, the DSA makes a blanket determination that the data protection law in a given foreign

---

[99] Norwegian Act of June 9, 1978 Relating to Personal Data Registers, para. 36, approved translation reprinted in Compilation of Privacy Legislation in OECD Member Countries, OECD Doc. No. DSTI/ICCP/79.11/14 (March 5, 1979), also reprinted in U.S. Dep't of Commerce, Selected Foreign National Data Protection Laws and Bills 145-67 (1978) [hereinafter cited as Norwegian Privacy Act].

[100] Id.

[101] Id. para. 37.

[102] See generally note 110 infra.

[103] Austrian Privacy Act, supra note 82, §§ 1, 32; Danish Privacy Act, supra note 81, §§ 1, 21(1).

[104] Id. § 3(2).

[105] Id. § 21(1).

[106] Id. § 21(3).

[107] Id. § 21(4).

country meets Danish standards, then the case-by-case licensing requirement need not be met.[108]

The Danish law also exempts from the licensing requirement TDF transmissions involving data stored in a data bank "which is found in Denmark solely for the purpose of undergoing electronic data processing."[109] The exception to the licensing requirement for foreign data may be explained in terms of a desire to minimize the resources necessary to achieve the privacy protection goals of the Danish Data Protection Act. While the exemption of foreign data from protection under the Danish privacy law does not have an obvious negative impact on the privacy interest of Danish citizens, it would be interesting to see how the law is applied in practice to data about Danish citizens.

The more compelling reason for the exemption is a desire to protect and encourage data processing activities within Denmark. The exception for foreign data indicates a desire to reduce impediments to the import of data into Denmark for storage and processing. Application of this exemption, however, would make it more difficult to harmonize Denmark's regulatory initiatives with those of other countries. The Council of Europe's recent treaty concerning the protection of personal privacy calls for harmonized levels of data protection as between signatory countries.[110] The Danish law seeks to deal with this problem by giving the Danish Minister of Justice power to suspend the operation of the exemption with respect to "other specified countries or specified types of [data banks]."[111]

### *F. Austria*

The Austrian statute's[112] provisions governing transborder data flow are more detailed than any other European privacy statute currently in force. As with a number of statutes previously discussed, the Austrian

---

108 Id. § 21(2).

109 Id. § 21(3).

110 Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, January 28, 1981, Council of Europe. Chapter III of the Convention, entitled Transborder Data Flows, reads as follows:

> (1) The following provisions shall apply to transfers across national borders, by whatever medium of personal data undergoing automatic processing or collected with a view to their being automatically processed.
> (2) A party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party.
> (3) Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2: (a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection; (b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

111 Danish Privacy Act, supra note 81, § 21(4).

112 Austrian Privacy Act, supra note 82.

enactment also requires approval of an administrative body, the Data Protection Commission (DPC), before data can be transmitted out of Austria. Prior approval of the DPC is required (1) whenever data cross the Austrian border for any type of processing outside Austria, even if the data are subsequently stored inside Austria,[113] and (2) whenever there is "direct access" to data stored on Austrian territory equipment outside Austria.[114] In addition, the DPC must be notified whenever any company operating in Austria processes Austrian data for foreign persons or companies outside Austria.[115] Such processing services are subject to prior approval by the DPC "where so provided by international agreement."[116] Finally, the DPC must be notified of all situations in which equipment on Austrian territory has direct access to personal data stored outside Austria.[117] These provisions constitute, collectively, a comprehensive regulation of all TDF links involving personal data between Austria and the rest of the world.

The burden of these provisions is limited, however, by exemptions: (1) for data transmitted to a country that affords such data legal protection comparable to the Austrian law,[118] (2) as provided in international agreements between Austria and other countries,[119] and (3) uniquely, "where the person responsible for the data processing is himself the person affected by the data transferred."[120] Since the Austrian statute defines the term "persons affected" as "natural or legal persons or associations of persons under commercial law,"[121] this provision exempts intra-corporate transmission of data from Austria.

The Austrian Privacy Statute also sets forth explicit criteria to be applied by a data processing authority in determining whether to grant permission for the transfer of data outside of the country. The statute provides that such approval shall be given if four criteria are met.[122] First, the transfer must not conflict with the public interest, specifically described as including obligations under international law.[123] Second, the transfer must comply with the rules applicable to all transfers of personal data[124] concerning the circumstances under which personal data may be disclosed. Third, the Commission must find that the transfer does not harm the interests of the person whose personal data will be transmitted out of Austria.[125]

---

113 Id. §§ 32, 34(1).
114 Id. §§ 32, 34(2).
115 Id. § 33.
116 Id.
117 Id. § 34(2).
118 Id. § 32(2)2.
119 Id. § 32(2)3.
120 Id. § 32(2)1.
121 Id. § 3(2).
122 Id. § 32(3).
123 Id. § 32(3)1.
124 Id. § 32(3)2.
125 Id. § 32(3)3.

The fourth requirement is triggered only when the transfer abroad is made by a service company that processes data for other clients.[126] In that event, certain additional safeguards applicable to all offerings of data processing services are incorporated by reference. This provision may, however, be satisifed by compliance through "adequate safeguards . . . agreed upon" by the parties to the transaction.[127] One writer recently suggested that private contracts be employed to ensure a sufficient level of privacy protection in the transferee country to satisfy the transferor country's privacy law.[128] Indeed, the Austrian statute seems not only to contemplate such private contractual arrangements, but in certain circumstances to require them.

The authors have been advised that American companies operating in Austria have encountered difficulties in transmitting data to other European countries for processing. We understand that the transmissions have been permitted to continue, however, where it has been demonstrated, to the satisfaction of the Austrian authorities, that the protections given the data under internal company procedure or foreign law meet the requirements of Austrian law. Apparently, this process involves a detailed examination of corporate procedures by Austrian officials.

### *G. The United Kingdom*

Reportedly, the British Government has recently decided to introduce in the Parliament privacy legislation that would apply to transborder data flows. The United Kingdom is a significant center of data processing activity, and British authorities apparently wish to demonstrate to other countries that there is no reason to be concerned about the protection of personal information transmitted to the United Kingdom for processing and/or storage.

### *H. Other European States*

At this time, there is no privacy legislation applicable to private transborder data flow in other European countries, such as Italy and the Low Countries. Although Luxembourg has recently enacted data protection legislation,[129] the law has thus far only been applied to data storage facilities operated by public authorities in Luxembourg.[130] Following the recent political scandal concerning certain Masonic Lodges, Italian authorities have issued regulations ordering the security police to take inventory of all data banks in the country containing personal

---

126 Id. § 32(3)4.

127 Id.

128 See Note, Contracts for Transnational Information Services: Securing Equivalency for Data Protection, 22 Harv. Int'l L.J. 157 (1981).

129 Luxembourg Data Bank Bill of March 31, 1979, reprinted in U.S. Dep't of Commerce, Selected Foreign Data Protection Laws and Bills 133-44 (1978).

130 See Hogrebe, supra note 76, at 40.

information.[131] The regulations specifically describe these listing requirements as a precursor to the drafting of privacy protection legislation by the Italian Parliament.[132] A data protection law is also under study by a Justice Committee in Belgium; many aspects of the proposed Belgian statute, however, are said to be unsatisfactory from a business point of view.[133]

## VI. Control of Foreign Investment as TDF Regulation: Canada

In 1978 a special investigative committee, created by the Canadian Government, issued a report entitled *The Implications of Telecommunications for Canadian Sovereignty*, popularly known as the Clyne Report.[134] The Clyne Report begins with the proposition that all aspects of Canadian telecommunications, including TDF, must be regulated by the Canadian Government to preserve Canadian sovereignty.[135] The Canadian Government has never officially endorsed the conclusions or proposals contained in the Clyne Report, however, and officials of the Canadian embassy have indicated to the authors that the Clyne Report cannot be considered a statement of Canadian policy with respect to TDF. The TDF policy was described by these officials to be still in a state of flux pending further consideration by the relevant agencies of the Canadian Government.

Nevertheless, Canada illustrates a situation in which controls over various types of foreign investment seem to have begun to reflect a specific concern about TDF. In 1974 Canada passed the Foreign Investment Review Act,[136] a statute designed to control foreign investment in Canada. Some members of the business community, however, have alleged that the statute has been applied in a particularly stringent fashion to foreign investment in the Canadian computer service industry. The case of Comshare, Incorporated (Comshare), an American corporation, which was unable to obtain approval of its plan to buy controlling interests in a Canadian computer service company in which it held a minority position, illustrates the tendency. The Canadian company, CSL, Ltd. (CSL), was formed by Comshare in 1968. In 1970, because of financing needs, Comshare sold its controlling interest in CSL to another Canadian company. The buyer was not a computer service firm, but rather an investment firm seeking to diversify its portfolio. In 1978, after CSL had established a successful position in the Canadian service market, Com-

---

131 See Declaration of the Ministry of the Interior, Department of the Security Police. Government Document N.558/6.D.1.2, Rome, September 18, 1981.

132 Id. at 4.

133 International Chamber of Commerce, Commission on Computing, Telecommunications, and Information Policies, Note on the Meeting of October 9, 1981, at 4, I.C.C. Doc. No. 373/7 (1981).

134 Canadian Dep't of Communications, Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty, Clyne Report (1979).

135 Id. at 2.

136 Foreign Investment Review Act, ch. 46, 1973-74 Can. Stat. 619 (1973).

share approached its Canadian partner with a buy-out proposal and the Canadian company agreed.[137]

In an effort to obtain approval for the proposed acquisition, Comshare made extensive disclosures to the Canadian Government concerning its own finances and development plans, as well as the finances and development plans of CSL.[138] In addition, Comshare agreed, in writing, to remain subject to continued reporting requirements in connection with any proposed reorganization or disposal of CSL's assets. Finally, Comshare committed itself to a detailed program of future expansion designed to benefit the Canadian economy. This proposed expansion would have included additional Canadian investment, training of Canadian nationals, transfer of technology to Canada, and a promise to begin the export of data processing services to countries outside Canada.[139] Despite these representations, the application was ultimately denied on the ground that the proposed acquisition would not be of significant benefit to Canada.[140]

Another example of the interrelationship between Canadian regulation of foreign investment and Canadian regulation of TDF is the recently enacted Banks and Banking Law Revision of 1980 (Canadian Bank Act).[141] The Canadian Bank Act is a comprehensive revision of Canadian banking law. We are concerned here, however, with only two sections of the Act, one pertaining to the chartering of foreign banks and the other pertaining to the maintenance of bank records. Under the Canadian Bank Act foreign banks can, for the first time, charter subsidiaries in Canada directly. International banking is perhaps the most information intensive of multinational endeavors.[142] Therefore, increased American banking activity in Canada in the wake of chartering opportunities would certainly increase the possibility that electronically-processed banking records would be stored or processed in the United States. Accordingly, the Canadian Bank Act contains provisions specifically designed to deal with such an occurrence.

Certain types of bank customer records must be maintained in Canada. These records must describe "for each customer of the bank on a daily basis, particulars of the transactions between the bank and that customer and the balance owing to or by the bank in respect of that customer. . . ."[143] In addition, banks are required to retain in either printed, film, or electronic form "all registers and other records required or authorized" by the banking law including "any entries, books, vouch-

[137] I.C. Reorganization Hearings, supra note 3, at 208-09.

[138] Id. at 234-47.

[139] Id.

[140] Id. at 251.

[141] Canadian Bank Act, 1980, c. 40 § 155 passim, Vol. 2, No. 7, Can. Gaz. III (1980).

[142] See I.C. Reorganization Hearings, supra note 3, at 337, 341, 377, 420 (letters from U.S. banking officials to Glenn English, Chairman of Government Information and Individual Rights Subcommittee).

[143] Canadian Bank Act, supra note 141, para. 157(4)(a).

ers, paid instruments, signature cards, signing authorities, . . . in the possession of the bank . . . ."[144] In the event a given bank chooses to maintain the required records in electronic form, the bank must store the data in Canada and maintain equipment there "that is capable of reproducing any required information in intelligible written form within a reasonable time . . . ."[145] It may be assumed that this final requirement will require maintenance in Canada, not only of electronically stored data, but also of the software necessary to retrieve such data for inspection. Finally, banks are required to "maintain and process in Canada, any information or data relating to the preparation and maintenance" of required banking records.[146]

Copies and extracts from required records may be processed outside of Canada under certain conditions. Such processing is only permissible where "the bank shall so inform the [inspector of banks] and provide him with a description of the nature of those copies or extracts maintained outside Canada and a description of the further processing of information or data relating to such copies or extracts outside Canada . . . ."[147]

The Inspector of Banks is then empowered to prevent processing outside Canada, if he becomes convinced that "further processing outside Canada . . . is incompatible with the fulfillment of his responsibilities . . . ."[148] The Act also empowers the Canadian Minister of Finance to suspend processing outside of Canada in the event that the Minister concludes "such further processing is not in the national interest . . . ."[149]

The standards to be applied in determining whether to allow TDF may reflect the differing motivations behind passage of the Canadian Bank Act. The Bank Inspector's power to prevent TDF arguably reflects the general purpose of the Act, *viz.* to protect the integrity of the banking system by ensuring that the Bank Inspector has sufficient access to bank records to perform his oversight function. The power given to the Minister of Finance to suspend bank-related TDF, however, appears to open the way for the Canadian Government to regulate data processing by banks as a means of achieving broader economic and political goals.

## VII. Future Directions

The pace of developments in this field is so rapid that much of what has been written above could be outdated by the time it is published. No crystal ball is required, however, to predict that the following trends will continue: (a) the rapid development and application of new computer and telecommunications technologies; (b) the introduction of new domestic and international electronic data, voice, and video services;

---

144 Id. para. 157(1).
145 Id.
146 Id. para. 157(4).
147 Id. para. 157(6).
148 Id.
149 Id.

(c) the restructuring of commercial activity in the data services/telecommunications fields as new technologies make it difficult to maintain old regulatory distinctions; (d) increased national actions and regulation affecting transborder data flows as governments take measures to protect personal privacy and national perceptions of security and cultural interests, to encourage the development of domestic computer and data processing industries, and to develop public data networks in competition with private industry; and (e) increased activity in international organizations attempting to come to grips with the real and perceived problems of transborder data flow.

During the past four or five years American industry has been critical of the government for not having "a policy" or an organization to deal with TDF issues.[150] The business community, however, has diverse interests, conflicting priorities, and considerable ambivalence about the role of the government in this evolving theatre of operations.[151] On the one hand, there is considerable reticence to embark upon the development of an international legal regime for TDF. The concern is that international agreements will result in more TDF restriction, rather than less.[152] This apprehension is understandable when one considers statements made by the French and others, relating the need for international agreements to the significance of TDF for the international division of labor and the distribution of wealth among nations.[153]

On the other hand, there is increasing demand in both U.S. business and government circles for new multi-national agreements to facilitate international services trade. The Reagan Administration is seeking agreement that "services" will be on the agenda of the General Agreement on Tariff and Trade (GATT) Ministerial Meeting to be held in Geneva in October 1982. Any such initiative is bound to touch upon important aspects of TDF. Data processing is an important service industry in its own right, and many other service industries, such as banking, insurance, and airlines, also are dependent on TDF. It remains to be seen whether the member states will be able to reach agreement on TDF related issues.

The executive branch is not the only branch of the United States Government engaged in TDF initiatives. The Congress is currently considering a broad based revision of the entire structure by which the federal government regulates communications.[154] A bill passed by the Senate prior to the settlement of the government's antitrust action

---

[150] See generally, I.C. Reorganization Hearings, supra note 3, at 337-420 (letters commenting on the International Communications Reorganization Act by various corporate executives).

[151] Id.

[152] Id.

[153] Madec, Aspects Economiques et Juridiques, 406 Problemes Politiques et Sociaux 5 (1981).

[154] See S. Rep. No. 170, 97th Cong., 1st Sess. 1-2 (1981).

against AT&T[155] gives the FCC authority to ensure that

> the entry of foreign carriers or foreign persons supplying telecommunications or information services, facilities, or equipment into domestic United States telecommunications markets [is] upon terms and conditions which are reciprocal with the terms and conditions under which United States persons are permitted entry into—
>
> (1) the foreign nation in which the operations of such foreign persons offering telecommunications or information services, facilities, or equipment is based; and
>
> (2) the foreign nation under the laws of which such foreign telecommunications or information services, facilities, or equipment operations are established.[156]

Traditionally, the United States has eschewed such "reciprocity" requirements in trade relations, but there are signs that this consensus is weakening. It would be far better if trade issues, including TDF, could be resolved without such measures. It is hoped that the services initiative in the GATT and restraints by our trading partners will afford a solution.

The United States has every reason to insist that the national and international policies that promote the free movement of capital, technology, and goods in the world economy apply equally to the transfer of information and to the supply of related services. Multinational enterprises will not be able to make the economic contribution that is their strength if they are unable to transfer information freely among their affiliates. Further, the United States is increasingly dependent in its foreign trade on the export of services and high technology, including data processing services. If the American economy is to retain its capacity to absorb the products of other nations, it will need access to foreign markets for the goods and services it can provide competitively. To protect these interests, the Government needs to ensure that our trading partners will continue to permit access to foreign facilities for data processing and storage and to provide economic telecommunications links for these facilities.

---

155 S. 898, 97th Cong., 1st Sess. § 238(a), 127 Cong. Rec. 11216 (1981). The AT&T case was settled on January 8, 1982. See N.Y. Times, Jan. 9, 1982, at 1.

156 S. 898, supra note 155, § 238(a).