

TRANSBORDER DATA FLOW DEBATE

B.M. GUPTA

S.P. GUPTA

*National Institute of Science Technology &
Development Studies, CSIR Complex at NPL,
Hillside Road, New Delhi-110012.*

The paper attempts to provide an overview of the current debate on transborder data flow. It is divided into five sections. The first section provides the definition and basic concepts of transborder data flow. Traces the recent developments in computer and communication technologies and the emergence of computer-communication networks. Describes the reasons and advantages in the international transmission of information. Lists out the broader issues currently under discussion in the transborder data flow debate. This is followed by discussion on the concern for these issues in different countries and how they are perceiving them in their national informatics policies in the next section. The next two sections describe the type and volume of data being transmitted and the various actors and participants involved in the transborder data flow debate. The final section discusses in detail the issues involved in the whole debate namely that of: personal privacy; national sovereignty, independence and power and the social; cultural, and economic issues arising as a result of international transmission of information.

1. INTRODUCTION

Transborder data flows are broadly defined as units of information transferred and processed in more than one nation state. A variety of similar terms such as "transnational data flows" and "transfrontier data flows" are also used. In Europe, the term "frontier" is preferred over "border". However "border" and "frontier"

seems to be interchangeable. The terms "data" and "information" are used synonymously in the transborder data flow debate. In the present context the "data" refers to a set of organised symbols capable of machine processing and transmission. "Information" implies a higher class of data intelligible to human beings. It will also be appropriate here to make a distinction between computer and communication technologies. Seitz[1] defines communication as an activity in which the quality of information is preserved without any alteration of its contents. Data processing, on the other hand, improves the quality of information by transferring or manipulating it. Transborder data flows occur when extraterritorial data processing functions operate at one or more than one termination point in a communication link.

The problem raised by transborder data flow finds its antecedent in the rapid developments and subsequent convergence of computer and telecommunication technologies. Over the last decade, rapid developments have taken place in computer and telecommunication technologies. Each of these separate developments in its own way has constituted a revolution in our capacities to handle and transmit information - at greater speed with greater precision, and with the capacity to deal with greater quantities of information. Computers, in less than two decades, have gone from large-scale centralised super-adding machines used mainly for specialised purposes, to worldwide network of shared systems. The main trends in this are still towards smaller, faster, and cheaper technologies. Recent

developments in micro-miniaturised circuits give enormous gains in the performance and reliability with dramatic decrease in size and costs. The microprocessors now rival in capacity and performance compared to room-sized computers of twenty years ago. As a result of these developments, the extended use of computers and their ancillary systems have pervaded many areas of human activities. Large areas of production, service, maintenance and routine information handling of all kinds have come under automated control. Such operations are today increasingly interlinked. This increasing interdependence of these systems in agricultural and industrial production, energy, transport and marketing management and financial operations has been characterised as a new symbiosis between human and machine. The impact of this new symbiosis has already been considerable on various activities of present society.

Similarly, telecommunication has developed through earlier telegraph, telephone and telex systems to a complex global network embracing all of these as well as radio, television, microwave and satellite relays, carrying personal messages; commercial, economic, political, scientific and military information. Taken together, the above two sets of technological developments constitute a core change in the sustaining basis of human society. It is not just the computer and its impact on telecommunication with which we are concerned here but with the convergence and interaction of these developments to create a radically new information and communication environment. The new environment has made possible the following things:

- i) Communication by data users and data suppliers can become instantaneous, inexpensive and ubiquitous;
- ii) Terminals in one country can communicate with other terminals or data bases around the world either on a real time or store or forward basis, without human intervention of any kind;
- iii) Communication and computer links can be used on a point-to-point or network basis and in either direction;
- iv) National and international information networks are emerging with having remote access to "host computers"; and
- v) Distance and geographical barriers are becoming virtually irrelevant in a cost or operational sense.

The most significant development has been emergence of the international information networks which are responsible for the international transmission of information. There are several reasons why data or information may be passed from one country to another. The owner or user of data may wish to share and control processing facilities or to make use of a central data bank. Often, there are considerable financial benefits and added convenience from such centralisation. Many organisations, of course, are inherently international whether in terms of their purchasing or selling or other trade, or whether they are a part of a corporation which operates in several countries. There are also certain activities which by their nature, can only exist if there is an international communication, e.g. international banking and credit, airline reservations; world meteorological cooperation. Similarly, the pooling of international resources and ideas for scientific and technical research are examples of the need for international communication for the furtherance of international cooperation. For all the reasons mentioned above, international data communication in one form or another is essential. International transmission of data are already producing substantial benefits for large international companies either through more efficient management or computer resource sharing. It has also facilitated international co-operation in many areas of scientific research, namely weather forecasting, oceanography, etc.[2].

The transmission of data over telecommunication circuits began in the 1950's, with the early establishment of airline and defence networks. The technology developed by these pioneering systems began to see its applica-

tions in mid 1960's in banking, corporate management, government, time-sharing bureaus and so on. The airline and defence network have had an international dimension almost from the beginning, but until the end of 1960's, other systems using data transmission were confined to a single country, with very few exceptions. The growth of international data transmission is thus essentially a phenomenon of the 1970's. The speed, accessibility, and interactive capability provided by developments in international networks do make a qualitative difference to the way in which data can be shared and used and to the interdependence of the parties at each end of the link. At the same time, the intangible nature of data transmission and the difficulties of monitoring what is being sent adds to the concern over possible misuse and undesirable cultural, social and economic effects. These concerns fall into following three broad areas:

- i) The privacy and security of personal and corporate data, particularly where it may be transported to or accessed from another country which may have low standards of privacy and security than the country where the data originate;
- ii) The increasing international independence created by sharing of data or computing resources between countries and the resulting vulnerability of one country to events or decisions in another which are outside its control; and
- iii) The danger of the concentration of data processing facilities in some countries, with a resulting loss of economic opportunities and capability. Furthermore the vulnerability of the concentration of data, both inside and outside of a country's boundaries, can pose a threat to its national security.

2. NATIONAL POLICIES AND CONCERNS

When the various countries in the world consider their information policy issues with which

they are faced, they must consider not only the domestic concerns, but also the implication of the international flow of data for their own situations. Broadly speaking these international concerns are focussed on:

- i) Major role played by the United States in the supply and use of information resources. At present 85 per cent of the world supply of computers and computer data is in the hands of 10 western companies and IBM provides almost half of it (Table 1)[3]. A bulk of data bases are also located in the United States (Table 2)[4]. These data bases account for 80 per cent of the worldwide transmission and processing of information. Also a considerable portion of official and government information relating to western European countries is held in USA data banks. There is a considerable fear that the existing trends, if unchecked will lead to an unhealthy American dominance over other nation's economic, social and cultural values. The European, Japanese and other Governments with substantial investments in domestic information industries have already begun to view the continued American dominance with alarm. These nations, being strongly apprehensive of the increasing dominance, now aspire to strengthen their own information sector for reasons of national prestige and more importantly, for the present and future trade advantages the information products and services might bring. Despite a growing manufacturing capability, these nations also fear the loss of domestic and foreign markets to American firms offering sophisticated information processing services. They are, therefore, now very much concerned to protect their local industry by augmenting and reorganising their indigenous resources and facilities.

Table 1

Turnover of leading informatics corporations, 1978

		In US \$m
17,000	IBM (USA)	
2140	Burroughs (USA)	
1970	Sperry Univac (USA)	
1868	Control Data (USA)	
1620	NCR (USA)	
1602	Digital (USA)	
1600	H.I.S. (USA)	
1590	Fujitsu (Japan)	
1066	611-HB (France/USA)	
1039	ICL (U.K.)	

Table 2

*Reference data bases and data base records :
Geographical distribution, 1975-79*

Area	(In Number)		
	1975	1977	1979
United States of America			
Number of data bases	177	208	259
Number of records (millions)	46	58	94
Other Developed Market Economies			
Number of data bases	124	154	269
Number of records (millions)	6	13	55
Total:			
Number of data bases	301	362	528
Number of records (millions)	52	71	148

- ii) In many instances the challenge is perceived not due to United States government but more specifically from the multinational corporations, which have acquired supranational powers and are independent of any local governments' control. The multinational corporations which are expected to account for 16-20% of the world output by 1985, are engaged in a substantial amount of transborder data traffic.

The concerns about transborder data flow vary from country to country. However, it is well documented in some reports commissioned and submitted in few countries namely France, Canada and Sweden. The French government has initiated a number of steps to ascertain the impact of data flow on French economy and citizens. The Norce-Minc Report of "L' Information de la societe"[5] submitted to the French Government in June 1978 is a comprehensive catalogue of French concern about the role of United States in computing, data processing and telecommunications. The report makes the following points.

- i) the "information of society" will have serious social, economic and cultural consequences for France;
- ii) foreign firms (primarily IBM) must not be allowed to be instruments of foreign (primarily United States) dominance;
- iii) Post, Telephone and Telegraph Administration should be restructured so that telecommunication can be re-directed to work more closely with other high technology agencies;
- iv) mastery of component technology is as important as nuclear mastery for national independence;

The above report represents a serious French commitment to retain or achieve control over the future information industry. The French Government prodded by the Norce-Minc report is also now considering alliances with other European administrations in the area of telecommunications, computers and electronics to combat American companies. In addition, the Government has set up a special commission on "Transborder data flow" in 1979 to report directly to the President of the Republic.

For the last ten years the Canadian Government has also been trying to establish and maintain an information-communication policy. As a result, a number of government reports have been produced in this area. The report entitled "Telecommunication and Canada"[6] popularly known as "Clyne Report" submitted in

1979 in particular considers the implications of transborder data flows for Canadian sovereignty. According to this report Canada is increasingly reliant on foreign (primarily United States) computing services. It stresses the need to avoid the dependence and reliance on American technology. The report suggests that the only alternative solution lies in the cooperative development of a national strategy to protect Canadian interests and derive the greatest benefit from the development and use of information technology available in Canada. To this end the Committee made two recommendations:-

- i) The Federal Government, in agreement with the governments of its provinces and the private sector, should stimulate the development of plans for the creation of Canadian-owned private data banks, as well as other similar agencies funded by government aid and other incentives should be devised for that purpose;
- ii) the government should act immediately to regulate transborder data flows to ensure that we do not lose control of information, vital to the maintenance of national sovereignty.

The report concluded that Communication technologies are developing so rapidly which poses threat to Canadian sovereignty in both its cultural and commercial aspects.

In Sweden the "Committee on the Vulnerability of Computer Systems"[7] which was set up by the Ministry of Defence at the behest of the Cabinet, under-scored several political, legal and economic problems, resulting from extensive computer use and foreign data flow. It stated that "vulnerability" is due to several factors: chief among them are dependence on foreign sources; and manpower dependence. The main cause of present vulnerability is that there has been no governmental control over the development which has led to the highly computerised society of today. There has been no overall assessment of the risks entailed in the entire field of civil sector, much less for the country as a whole. The lack

of awareness of vulnerability problems is not unique in Sweden. There are several other countries both developed and developing, which have recently shown concern over the problems of transborder data flow. Some of these countries have been expressing these concerns at the various international forums, conferences and meeting, etc.

3. TYPE OF TRANSBORDER DATA FLOW

Before debating on the various issues and factors involved in transborder data flow, it will be worthwhile to know what type of data flow are actually involved. There are four types of data that are considered under this area. They are: operational data, financial data, personally identifiable data, and scientific and technical data. Operational data consists of those transborder data flows that support organisational decisions or that sustain certain administrative functions. In this area most of the international data flows normally consist of flows between subsidiaries and headquarters of multinational organisations (corporations, trade unions, and others). In such cases, data from subsidiaries are usually processed by the headquarters computing facility. Operational information maintains vital lines of communication between parent organisation and its subsidiaries. The firms that maintain operations in more than one country and depend upon data communication links to aggregate and to disperse management information may be particularly vulnerable to restrictions on data flow. Restricting the flow of operational information is, therefore, a strong measure that can directly influence economic activities. The second category of data involves actual financial operations that result in credits, debits and transfer of money. It is important to distinguish operational data containing financial information from those data that represent actual currency transactions. The free flow of financial data permits concurrent financial arrangements and flow of capital conversely. Restrictions on financial data flow can, however, inhibit trade substantially, with economic consequences. A third type of data flow transactions is that which contains a personally-identifiable information. This informa-

tion may relate to credit, medical history, criminal record, employment, travel reservation or it may simply be a name or identification number. There is no accurate estimates of the proportion of personal data in international flows, but it is now recognised as being small, almost certainly less than 10 per cent. Although personal data is insignificant in the total volume, it has achieved widespread attention because it raises important issues which are different from those arising in other categories. The presence of personal information may require substantially different treatment due to the restrictions imposed in some states by legislations. A final type of data flow contains scientific and technical information. These data might include the results of experiments, surveys, environmental or meteorological measurements, etc. Bibliographical data bases and the scientific software to process raw data are also communicated to the multinational and scientific community by computer. Inclusive policies can promote scientific cooperation and assist in technology transfer, while exclusive policies deny these resources to various groups and nations [2,8].

3.1 Volume of Data

Although it is not possible to identify fairly well the type of data flowing internationally, very little estimate is yet available about its volume or the pattern of traffic. For the moment, there are only individual examples to quote. Societe Internationale de Telecommunication Aeronautique (S.I.T.A.) network carries some 100,000 million characters per year. There is also some world-wide figure including considerable volume of message-switched telegraph type traffic available. Such information as is available suggests that big networks have flows of the order of 10,000 to 100,000 million characters per year. A good many more have flows in the order of 1,000 to 10,000 million characters per year and below that level it is hard to justify the cost of even a single point-to-point international telephone line. In order to get a better idea about the volume and pattern of traffic the projected data communication

study to be commissioned for the European PTT's by the Eurodata Foundation will go a long way.

5. ACTORS AND PARTICIPANTS IN TRANSBOARDER DATA FLOW

The major actors in transborder data flow are national governments, industry, international and inter-government organisations. Each actor has some ability to influence the flow of information. Each actor perceives benefits by pursuing either exclusive or inclusive policies over the access, control and use of transborder data flow. Competition between the exclusive interests of information control and the inclusive interests of unrestricted transfer of information across national boundaries is the centre of controversy of the transborder flow debate. Inclusive interests represents the free flow of information. They want to promote increased sharing, use and exchange of transborder data flows. Exclusive interests on the other hand represents "Sovereignty over information". They want to promote controlled use and restricted access.

4.1 National Governments

The national governments are and will remain the most significant actors in transborder data flows. They take various roles in addressing the problems raised by transborder data flows: that of the governing policy-making authority; that of a user of information resources in each country; and that of supplier in most countries, of telecommunication facilities.

Major transborder data flow policy issues must be addressed at the governmental level. No fully adequate tradition for dealing with these matters exists, and yet there is a growing awareness of their importance. The broadest aspect of government involvement, then, is that of policy-making authority, with a wide variety of concerns of a political, economic, social and cultural nature.

The government has been the largest user of information resource including computing, data processing, telecommunication facilities and services. Usually the single largest customer for these resources, the government is and should be concerned primarily with cost availability, re-

liability and other ordinary commercial incidents of market place.

The national government, as a supplier, complicate matters even more, with the telecommunication being a government monopoly in most countries (The United States being the Chief exception). Historically, the Post, Telephone and Telegraph Administrators (PTT's) have led the classical life of the protected monopolist who can ignore market considerations and especially customer preferences more or less at will. In recent years there has been growing tension between many PTT's and their larger customers, often multinationals, who use modern electronics to configure on a cost effective basis the raw circuits provided to them by the PTT's. Private line circuits or communication channels dedicated to a particular customer have been the backbone of most international data networks[9].

4.2 *Industry*

There are various categories of actors involved in this section. In the first category falls the suppliers of goods and services used in the information field such as computer manufacturers, software suppliers, providers of data base services, and terminal equipment manufacturers. The second category consists of primary commercial users of such services namely multinational enterprises, commercial airlines, direct mailing companies, credit firms, energy suppliers, and manufacturers. The multinational corporations play the key role. They are both principal suppliers of necessary infrastructure and users of infrastructure, be it for corporate management purposes or for the provision of international data processing and information retrieval services. In fact corporate transborder flow takes either through intercorporate channels or among corporations in closed user-group networks.

The third category of actors are some of the enterprises which own and operate communication facilities. There are number of private communication carriers and international data network organisations. Various communications carriers are permitted to transfer computer-related data through inter-

national networks. Examples of this category are RCA Global Communications, ITT World Communications, and Western Union International which offer such services to selected countries. Transmission rates and reliability both tend to be lower through these carriers. Therefore, these services are not widely used. As far as international data network organisations are concerned, they are normally owned and operated by a group of subscribers for some common usage. Examples in this category can be of S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication) an International banking network and the S.I.T.A. (Societe Internationale de Telecommunications Aeronautique), an international airlines network. The previous banking network is owned and operated by a consortium of banks. It links nearly 600 banking organisations with close to 1000 branches in 17 countries of Europe, Canada and Brussels and Amsterdam and carries 120,000 messages daily for customers: tariff transfer, bank transfer, foreign exchange, interest payment, deposits, confirmation of debits and credits, and other statements.

The fourth category of actors are enterprises known under the label of "Data Processing Bureaus". They provide data processing, storage and retrieval services. Examples in this category are COMSHARE, CYBERNET, INFONET, MARK-III, TYMSHARE (The parent corporation of TYMNET). These bureau offer their powerful and highly sophisticated hardware for two major types of services: time shared data processing and data-base information retrieval. In addition, they provide complex software package which are often directed to highly sophisticated needs, and frequently allow access to large data bases. Since these services are offered on a cost-shared basis and with all the necessary in-house expertise and support capabilities, many organisations find them cheaper than to maintain their own computer and telecommunication capabilities.

In the fifth category falls those enterprises, which combine both the functions of private data networks and data processing services bureaus. They have recently emerged and popularly known as value-added networks. Such networks serve two functions: that of leasing com-

munication lines from other communication carriers and adding enhanced data transmission capabilities dedicated to data transmission for processing, storage and retrieval purposes. Such networks operate both on a regional level such as EURONET as well as in international framework such as TELENET and TYMNET. The last two are so far the only publicly accessible inter-continental networks that exist today. A number of such network services are planned for 1980's also. They include Satellite Business Systems (SBS) and Xerox Telecommunication Networks. American Telephone and Telegraph Company (A.T. & T.) has also plans for an advanced communication services to compete with these new data networks.

4.3 *International & Inter-Governmental Organisations*

These category of organisations play a significant role in transborder data flow debate. Their, actual use of computer communication is probably quite small; however, these organisations provide an arena both for controlling data communication technology and for debating and resolving conflicts about the transborder data flow directly as well as indirectly.

One of the main inter-governmental organisations in this area is International Telecommunication Union (I.T.U.), a specialised agency of the United Nations. Although the I.T.U. operates no communication facilities yet its planning, standard setting and coordination functions extend to telephone, telegraph, broadcasting and data communication. Most of the permanent work of the I.T.U. is performed through its International Telegraph and Telephone Consultative Committee (C.C.I.T.T.), and the International Radio Consultative Committee (C.C.I.R.). Administrative conferences held under I.T.U. sponsorship have considerable authority to establish important international practices, such as the allocation of radio spectrum frequencies, etc.

The I.T.U. has not directly addressed transborder data flows issues but has dealt increasingly with setting standards and tariff principles for international data networks. There are also a number of regional telecommunication organisa-

tions such as the Conference Europeenne des Administrations des Postes et des Telecommunications and the Asia-Pacific Telecommunity, which attempt to coordinate the regional planning of facilities and to promote other cooperative activities. One international organisation also serves as a carrier of international telecommunication traffic and operates its own system of communication satellites. It is the International Telecommunication Satellite Organisation (I.N.T.E.L.S.A.T.).

A number of similar other organisations which have been directly involved in the debate are: The Council of Europe, Organisation for Economic Cooperation and Development (OECD), The European Communities, the Inter-Governmental Bureau of Informatics (IBI), etc. The Council of Europe started the work on privacy aspects of the medical data of individuals in the early 1970's. In 1973 and 1974, the Committee of its Ministers adopted two resolutions concerning the privacy of individuals vis-a-vis electronic data banks in the private and public sectors respectively. The subsequent work of the Council in this area ended up in a treaty to deal with the broader issues of personal privacy. This treaty places obligations on data users and confers right of privacy on data subjects, and it allows a country with national privacy legislation to restrict data flow only to countries where no equivalent legislation exists. The O.E.C.D. interest in transborder data flow started as early as 1969 as a result of its report in 1971 on privacy protection. In July, 1974 it organised a seminar on policy issues on the protection of privacy. In order to obtain more evidence on the nature of problem, O.E.C.D. organised a broader seminar on the theme "Transborder Data Flows and the Protection of Privacy" in September, 1977 at Vienna which discussed the broader aspects, notably taking into account the recent development in data networks. Subsequent to the Vienna symposium, a new High Level Expert Group on Transborder data barriers was created in the early 1978. This group subsequently developed guidelines which are intended: to bridge between the privacy protection situation now developing in many European countries, and the one developing in non-European O.E.C.D. Member coun-

tries; and to create a more homogeneous international data regulation environment. The European Economic Community, primarily a geo-political organisation has mainly concentrated on economic and trade aspects of the question. It has carried out studies concerning the problems of harmonisation of national legislations within the community, the problems of data security and confidentiality, and the nature of transborder data flow. A Sub-Committee of the European Parliament held a public hearing on data processing and the right of individuals in early 1978. Its work has resulted in placing to the European Parliament in spring 1979 a report which was subsequently adopted by it in spring 1979. Subsequent work of the community has given some consideration to the drafting of a Directive to create a community for the exchange of data among countries. The International Bureau of Informatics (I.B.I.) an European and Third World Trade oriented group, has also considered transborder data flows, though largely in the context of Third World concerns.

The United Nations has been indirectly concerned in transborder data through its "Committee on Peaceful Uses of Outer Space". However, UNESCO has shown concern in this question which has been mainly concentrated on mass media aspects of transborder flow. Its recent Mc Bridge Commission Report, has, however, dealt with data question. This report calls for an assessment of overall traffic structure of the international data transmission that presently discriminates against developing countries. It advocates better access to satellite collected data on earth resources, crop growth, ore deposits to developing countries from developed countries. There are other organisations also, which have from time to time dealt with these questions, namely, Nordic Council and various non-governmental organisations such as the International Federation for Information Processing (IFIP), Inter-governmental Council of Automated Data Processing (ICA), etc.

5. BROADER ISSUES INVOLVED

5.1 There has been growing public concern, especially on the international transmission of

personal data. These public fears have persuaded many governments that special legislation is required to regulate the use of personalised data. Of the OECD member countries, more than one-third have so far enacted one or more laws, which among others are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriations. In the federal states laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" whereas in English speaking countries they are usually known as "privacy protection laws". The debate about data flows goes further than privacy. Countries are often worried that they are sending too much information to foreign nations for processing or that they rely too much on outside countries for other computer services. Therefore, they may on purely technical grounds use their privacy laws to restrict the movement of data.

In the United States there are many privacy acts at the national, state, and local level and considerable attention is paid to the private issues within the private sector. The U.S. States have drawn these laws without referring to data processing as such: privacy protection is regarded in the United States as the civil and human rights issue not one of economic and industrial regulation. The U.S. policy on the personal privacy aspects of transborder data flow is built around the notion of free flow of information and the desirability of maintaining that free flow so far as possible and so far it is compatible with other human rights.

A number of countries namely: Sweden (1979), West Germany (1977), Denmark (1978), Norway (1978), France (1978), Austria (1978), Luxembourg (1979) besides Australia, Canada and New Zealand, have enacted laws in this direction. These laws have a number of common features. Nearly all of them place restrictions on the export of personal data and usually demand the existence of comparable law in the recipient country. These are limitations on the length of time data can be stored, and regula-

tions on secondary use, sharing and dissemination of data. There are remarkable differences in the United States and European laws which are:-

- i) Europe has chosen the "Omnibus" approach: as comprehensive regime of public law. The U.S. has opted for a series of privacy laws that cover different subjects. Relevant laws concern: credit registration (1971), federal data banks (1974), and student records (1975);
- ii) In European countries, the existing privacy laws cover the public as well as private sector, whereas in USA and Canada, mostly the public sector is subject to privacy legislation so far;
- iii) Most European Governments have adopted some form of government machinery to monitor the implementation of their privacy protection legislation; in the USA on the other hand, no special federal agency or commission has been created;
- iv) In USA, most of the privacy laws refer to physical persons only. However, recent laws passed by some countries in Europe cover legal entities i.e. such as multinational corporations. This enables a country to relate industrial, financial and commercial information as well as personal data. Norway, Austria, Denmark and Luxembourg have all extended their privacy laws to cover legal entities, while France succeeded to pressure from multinationals on this point and restricted the law to physical persons for the time being.
- v) Additionally United States laws apply only to its country's citizens while in Europe, reciprocal agreements among nations provide protection for the citizens of all participating countries. This asymmetry could prevent the United States from obtaining information from foreign countries.

Some limited progress has been made in developing guidelines to coordinate conflicting national legislation. The OECD has set up such guidelines, but they are voluntary, and several countries are reluctant to enter into the agreement. The guidelines attempt to reconcile some basic differences between United States and most European Nations. Outside the OECD, the Europeans have adopted a binding treaty within the Council of Europe. The treaty placed obligation on data users and confers right of privacy on data subjects and it allows a country with national privacy legislation to restrict data flow only to countries where no equivalent legislation exist[10,11].

Although privacy laws have been widely discussed over the last few years, but the international transmission of personal data is very small except in banking, credit control, travel application, etc. It is generally observed that a great deal more transborder traffic relates to sensitive corporate information. This data is as sensitive as personal data. Transborder data flows restrictions are not limited to industrial nations alone. Increasingly, less developed countries fearing "electronic colonization and electronic imperialism" have adopted the right to exercise the control over all information gathered within the borders of national-state. According to a recent survey of Inter-Governmental Bureau for Informatics (IBI) a number of developing countries have indicated their intension to regulate the transborder data flows. While considering individual countries, Brazil is the only developing country which has the most sophisticated legislation. Imports of computer and data services are closely scrutinised by the government and prior approval must accompany all export. It grants only temporary authorization for access to its information sources. It is also contemplating the creation of national register of data banks and applying tariffs on information services. In other developing countries namely Venezuela and Algeria, there is an embargo on the foreign movement of data related to oil production. Mexico has put a condition that their foreign flow of information of Mexico origin be subject to rules that regulate the

circulation of information on grounds of national interest[12].

5.2 *National Interdependence, Sovereignty and Power*

The international transmission of information does lead to national interdependence in many situations. The advantages of using remote data processing facilities for sharing expensive facilities had led to situations where users in one country become dependent on the reliable operation of facilities in another. For example several national airlines use seat reservation systems belonging to and located in a foreign country (e.g. AIR IRAN uses the KLM computer in Amsterdam)

Another example of this type can be seen in the case of computerised banking system called S.W.I.F.T. (Society for World Financial Information Transactions). This system allows finance houses to buy and sell in world market and to make loans anywhere at any time. It means that money can be moved around the world with greater rapidity and without any physical or legal hindrance. S.W.I.F.T. handles 300,000 transactions at a time, some of considerable size beyond all national control. This system generates a kind of "stateless money" huling around the globe potentially creating international currency instability as it moves. In the hands of a hostile power, S.W.I.F.T. could be devastating tool. Besides increasing the velocity of international money and causing currency and stock fluctuations, such devices could create a kind of electronic "free port" where funds can be placed in unregulated market [2,13].

Fears have also been expressed that as national interdependence increases the activities of a country to control its own affairs will be reduced, thereby infringing on its sovereignty. Certainly the increasing influence of multinational companies in the trade and industry of many countries has resulted in data relevant to day-to-day functioning of a country being held outside its borders. If this data is withheld for some reasons then the industry and trade of the affected country may be put at risk. Furthermore, if the multinationals hold vital data relating to the operations of the

company in distant computers then the ability of a government to direct the operations of that multinational in its area of authority is reduced.

Also once the data is exported they often move outside the jurisdiction of domestic courts of law. Sometimes national sovereignty interest may compel disclosure of information contained in transborder data flows or may order denial of such flow. Data communication networks are vulnerable to interceptions and contents of their transmission can be disclosed to unauthorised parties. Valuable interelligence is gathered from monitoring such communications and surveillance is performed routinely by countries who want to learn about the activities and groups in their own countries.

The misuse of data for political purposes constitute another important facet of national sovereignty. Threats of economic sanction may in future be an increasing common international means of pressure to attain political aim. If a country is highly dependent on imports of computer equipment and services, automated data processing (ADP) sector may become an attracted target of attack in different forms of economic warfare. Even a limited blockade against the import of spare parts would very quickly have serious affects.

Another spectacular example in this field is that of remote sensing by photo satellites. These satellites (spies in the sky) are used to survey the earth and its diverse features including agriculture, forest, ocean and mineral resources. A large amount of data is regularly collected about various countries through these satellites. At present, only few countries namely United States, Soviet Union, etc have the capability of making and launching remote sensing satellites on one hand and the processing electronically the data collected by these satellites on the other hand. The differential capacity to sense the earth and interpret the data has placed many countries at a serious disadvantage. On the basis of technological supremacy the United States has developed large data bases on the resources of developing countries. The United States launched the "LANDSAT Program", consisting of a series of satellites under the auspices of National

Aeronautical and Space Administration (NASA) in 1972 as a part of broader resource monitoring and assessment system. To-date the raw data secured from remote sensing has been made available by the United States government to other governments at a nominal cost. However, the processed data is handled quite differently, normally treated as "proprietary information".

This form of data gathering through remote sensing poses two issues both affecting national sovereignty. First, there is a basic inviolability of national space. Second, there is an unequal capability to use the data derived from remote sensing. As one report carefully notes "there is a little doubt that sophisticated institutions can use remote sensing technology to increase the economic and political power relative to less sophisticated institutions. Knowledge of likely oil deposits, projection of crop yields and better estimates of mineral concentration can help developed countries and their multinationals possessing remote sensing technology to make better political judgements, rewarding bids in international market and better bargaining position vis-a-vis developing countries". Consequently, we find that many multinational governments in satellite venture. An example of the category can be seen in the United States "Stereosat Spacecraft", to be funded jointly by the United States government and its petroleum and mineral multinationals. Also the growing usefulness of remote sensing technology has made the United States multinational corporations to push for shifting the LANDSAT System from under NASA to private ownership. The French too are seeking to enter the market for remotely sensed data. They have recently formed a company SPOT-IMAGE which will acquire, process and sell remotely sensed data. In the future a large number of companies are likely to enter in this field[14, 15].

5.3 *Economic Issues*

There are important claims that certain national policies in transborder data flow regulation have economic and trade under-currents. A clear idea of this economic under-currents can be had from a report entitled "Telecommunication and

Canada" brought out in 1979 by Canadian Government. According to this report Canada is increasingly reliant on foreign, primarily United States computer services. When 400 Canadian subsidiaries of United States companies were approached it was found that in 1978 some \$ 300-350 million dollars worth of computer services were imported from United States services headquarters, with an increase of about \$ 15 million estimated by 1985. Further it was expected that as a result, about, 23,000 jobs in computer services will have been lost to the Canadian economy by that time. This has led to the potential of growing dependence than independence in the development and utilisation of advanced information technology, the loss of employment opportunities in addition to balance of payments possibilities.

The transfer of employment which result from foreign data processing is more than short term loss, it is contended. However, these threats to employment hit hard at a period when the countries have large number of people without jobs. They influence governments to either reduce foreign flows or impose taxes (VAT) or tariffs (for lost domestic business) on enriched data which is processed and then returned to the originating country. Concerns along with these lines were also made by a number of countries. They think that setting up of an international information trade could disturb "balance of payments" in a way which would be difficult to handle, given that these exchanges do not appear in custom statistics. They mentioned the fact that information being intangible is not identified in trade statistics. Therefore, its economic dimensions are not measured by the major international organisation (World Bank, OECD, etc.). When more of the implication of the information economy, are known, new approaches to the taxation of domestic and foreign information services will become more clear. At present, however, many countries are still trying to decide how to tax software, magnetic tape, disc packs and cards[12].

5.4 *Social and Cultural Dimensions*

With regard to socio and cultural aspects, serious concern has been expressed about the potential of cultural domination from one country by

another or from one region by another. This risk is perhaps greatly exaggerated since experience shows that opening up to the outside world is usually accompanied sooner or later by a sustained determination to maintain one's own cultural values in the face of imported alternatives. It is, however, worth pointing out that "culture industries" from newspaper to music business, and even to banks of data are particularly obgopolitics and prone to domination by certain groups and values. The removal of barriers can therefore, lead to cultural imperialism which sometime-accompanied model of imported development. Even if we look within the narrow sense of transborder flows (ignoring TV, etc.) the use of foreign computer aided learning programmes and use of foreign videotex, home service may emphasise foreign products, values and cultures.

REFERENCES

- [1] Seitz. Data communication and data processing - A basis for definition. Telecommunication Policy 1980, (March), 49p.
- [2] Organization for Economic Cooperation and Development. The usage of international data networks in Europe. Paris, 1979.
- [3] Hurtado, M E. Tug of war over computers. South 1978, (January), 28-29.
- [4] Williams, M E. Data bases and on-line statistics for 1979. Journal of American Society of Information Science 1980, 7 (December), 27-29.
- [5] Nora, S and Minc, A. Report on the computerisation of society. MIT Press, 1980.
- [6] Canada, Department of Communications, Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty. Telecommunication and Canada. Ottawa, 1978.
- [7] Sweden, Ministry of Defence. The vulnerability of computerised society: considerations and proposals. December 1979.
- [8] Novotny, E J. Transborder data flows and international law: a framework for policy oriented inquiry. Stanford Journal of International Law 1980, 15 (Summer), 181-200.
- [9] Fishman, W L. Introduction to transborder data flows. Stanford Journal of International Law 1980, 15 (Summer), 1-26.
- [10] Hondius, F W. Data law in Europe. Stanford Journal of International Law 1980, 15 (September), 87-112.
- [11] Kuitenbrouwer, F. The World data war. New Scientist 1981, (3 September), 604-606.
- [12] Pipe, Russell. Transnational data flows. Inter-Media 1979, 7(6), 12-16.
- [13] The Stateless money. A new force in world economics. Business Week 1981, (21, August), 76-85.
- [14] O'Brian, R.G. & Hellencir, G K. The political economy of information in a changing international economic order. International Organization 1980, 34(4),
- [15] Schiller, H I. The transnational corporation and the international flow of information: Challenges of national sovereignty. Current Research on Peace and Violence 1979, 11(1), 1-11.