Interdepartmental Task Force on Transborder Data Flows : background papers

WORKING COPY ONLY

Interdepartmental Task Force

on Transborder Data Flows

1. [Background papers]

A Discussion Paper Based on the Work of the Sovereignty Aspects Working Group

Mar 83 version
contains "conclusions"
in TBDF binder

Prepared by: J. Knoppers

September 1982

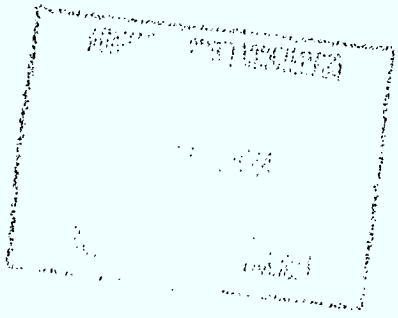

TABLE OF CONTENTS

REPORT ON SOVEREIGNTY ASPECTS OF TRANSBORDER DATA FLOWS

1. INTRODUCTION

1.1 Background

The last five years have seen a quickening in the pace of the computer/communications revolution. Especially important is the fact that new products and services are being introduced to the market place at such speed and to such a degree, that they are already having a noticeable effect on society. Of equal, if not greater importance, is the fact that the convergence of computer and communications technology has become a practical reality, not just in the technical sense, but also in many aspects of the daily life of society. In the past, if the introduction of new production processes, products and services made possible by new technologies, and their impact on society, led to problems, these were handled internally by the nation-state, as they were primarily matters of a domestic nature. International issues, when they arose, were related to questions of trade balances, access to natural resources, access to markets and access to the new technologies.

The convergence of computer and communications technologies as well as recent developments and applications, has had a two-fold effect:

- it has created a number of new activities for which no policies exist or, the development of which, existing policies frustrate; and,
- it has led to an urgent need to review existing policies not only because their efficacy has become questionable but because this convergence has created policy conflicts. Policies relating to data transmission (communications) and data manipulation (computers) were put into place before the advent of a converging digitized "wired society" and were compartmentalized according to the technology used, either through the physical product produced (e.g., newspapers, records, films, etc.) or the manner in which they were transmitted (e.g., broadcast, telephone, telex, postal services, etc.).

Normally, these would be domestic concerns only were it not for the fact that this convergence of computers and communications is developing as rapidly among countries as within individual countries. The rapid rise of networks of interconnected computer systems and data transmissions on a world-wide basis has, therefore, rendered traditionally domestic issues, international in effect.

In addition to the interconnection of national communication networks, the rapidity with which growing volumes of data are flowing across boundaries, and the "non-physical" nature of these data flows, have made obsolete or irrelevant many of the traditional methods whereby a country maintained its sovereignty. Finally, the ability of the new technologies to collect, vast quantities of data has led to new concerns related to legal questions,

cultural impacts, vulnerability, dependency and confidentiality, of which the protection of personal data (privacy) is one very important sub-set.

It is, therefore, not surprising that individual countries and international organizations are placing increasing amounts of emphasis on their attempts to understand and come to grips with the economic, legal, cultural and social complexities raised by what has come to be known as the information age.

The rapid advances in computer/communication technologies; their convergence and their continuously widening application; their increasingly important role within society; as well as the increased links and interdependencies they create between societies, have on the whole had a positive effect and brought many opportunities. On the other hand, concerns have been raised about possible negative impacts which, if they are not adequately understood and dealt with, might outweigh these benefits. In order to address these concerns in the Canadian context an Interdepartmental Task Force, consisting of a Steering Committee and three Working Groups, was established.1/ Extensive consultations were carried out with Canadian industry.

1.2 **Purpose**

In line with the terms of reference of the Task Force, the mandate of the Working Group on Sovereignty Aspects of Transborder Data Flows was to:

- develop a conceptual basis and approach;
- establish an analytical framework;
- identify broad subject areas of concern and vital considerations; and,
- collect and prepare factual information.

The concept of transborder data flows arose in part as a generic term to cover issues, as well as real and perceived problems, arising from movements of electronic (basically digitized) data across national frontiers through linked computer/communications networks. Its impact on "national sovereignty" considerations is a natural focus of any analysis of this concept.

The working definition of transborder data flows is as follows: "electronic or machine-readable data or instructions which are transmitted or move across national boundaries for purposes of processing, storage or retrieval in most cases utilizing computer-communication systems and interfaces".

In the context of the work undertaken by the Task Force and in consideration of other activities currently underway in the federal government, certain TBDF-related issues are not being addressed in full at this time. The exclusions are:

Video and Voice

Although video and voice transmission are part of TBDF, they have not been reviewed in detail because the federal government already was well along in the process of developing new broadcasting, cable TV and satellite use

policies when the Task Force was established. Cultural issues are addressed in this report in a narrow sense so as not to duplicate work being carried out by the Federal Cultural Policy Review Committee.

Privacy

One of the most sensitive TBDF areas is that of confidentiality of data flows and data use and, in particular, data on or about individuals, i.e. privacy. During the past decade privacy concerns have dominated the discussion of TBDF. Only recently have economic and national sovereignty concerns received attention. In order to provide a clear focus on these other TBDF concerns, it was decided to temporarily set aside the privacy question. It should be noted that the federal government has recently passed a new Privacy Act (included in Bill C-43) to replace the privacy provisions currently in force under Part IV of the Canadian Human Rights Act. As a result, the federal government is revising its privacy practices and procedures to comply with the new legislation.

A few words are necessary on the use of the term "sovereignty" in this paper. There is no broad and internationally agreed upon definition of the term "sovereignty". In its proper sense, the term "sovereignty" is a relatively narrow legal concept, and as such is discussed in some detail under the section on "Jurisdictional and Legal Issues". National sovereignty concerns in the context of TBDF, however, go considerably beyond that narrow concept, touching upon a wide range of cultural and vulnerability considerations. In relation to other issues discussed in this report, therefore, the term "sovereignty" is used to designate the practical ability of Canada,

- to protect itself and its citizens from encroachment from without, i.e. the protective or defensive element; and,
- to develop and effectively implement its economic, cultural and social policies, i.e. the positive element.2/

1.3 Scope, Organization and Work Program

The growth of transborder data flows and the unique nature of these flows have raised a number of broad sovereignty issues both internationally and domestically and past and current discussions on TBDF cover a wide range of concerns. While a number of specific incidents of a TBDF nature have been reported, so far they generally have been rare and isolated. This has not dampened concerns but rather seems to have stimulated further discussion and speculation causing one commentator to conclude that "transborder data flow discussions are a prime example of hyperactive imaginations being fuelled by insufficient knowledge". Yet the incidents that have occurred are real,3/ actions have been taken by various countries, and uncertainties about the applicability of the current laws and regulations to the new computer/-communications technologies do exist. Preliminary information now becoming available has raised valid concerns within the public and private sectors, while certain new computer-communication technologies are moving faster to becoming daily realities than was thought practical only a few years ago.

A number of these concerns can be readily classified:

- legal and jurisdictional aspects;
- cultural impacts including information retrieval services;
- vulnerability concerns; and
- data storage and retention requirements.

These areas of concern were made the subject of five sub-groups led by various members of the Working Group.4/ The focus and scope of each of those sub-groups were as follows:

° Legal and Jurisdictional Aspects

This project examines some of the legal questions associated with the issue of transborder data flows including domestic legal issues associated with the use of the computer in the area of criminal law; existing legislative requirements concerning evidence and records; "proprietary" rights; "liabilities"; patent and copyright; and specialized areas such as banking and securities law. Other areas which were investigated include potential international aspects of domestic legal issues; concepts such as "sovereignty" and "jurisdiction" and the implications of TBDF for traditional formulations of these concepts; the rights of states under international law to control information beyond their borders or to control the flow of information from their territory; and potential relevant international legal instruments.

° Cultural Aspects

The project report analyzes current government policies and mechanisms designed to protect, ensure the survival of and stimulate Canadian cultural products and heritage and the relevance and applicability of these policies and mechanisms to computer/communication-based cultural entities. In particular, the status of the electronic cultural heritage (machine-readable data files, and electronic cultural products, on-line public data bases) were examined in detail.

° Public On-Line Information Retrieval Services

A first step in the analysis of network information services, this report was a joint project with the Economic Aspects Working Group. This study was to provide a descriptive qualitative profile of public on-line information retrieval services not only in terms of order of magnitude assessment of the size and growth trends but also of legal concerns of the industry and cultural relevance. Pertinent developments in this industry in the U.S. and Europe were also investigated.

° Vulnerability Issues

This project examines the characteristics of advances in computer and communication technologies in terms of their vulnerability to misuse. In particular, concerns have been raised about fraudulent use or misuse of computer/communication systems and the data in those systems from remote

locations. Specific items included computer security, network reliability and robustness, and contingency planning in relation to TBDF questions. Other areas examined included remote sensing, electromagnetic pulse, the role of information as a valuable resource and vital cog in the delivery of services, increased interdependencies between national, international computer/communications systems and dependencies on data flows and integrated systems and new services as well as an analysis of the role of national boundaries in computer/communications networks.

° Data Retention and Data Storage

This project reviews current federal government data retention requirements and, in particular, with a focus on attendant locational requirements, if any. The question of how records are stored in light of the requirements of the Canada Evidence Act, the possibility of data retention requirements allowing for data storage in machine readable form with remote access and resulting TBDF implications were also examined. Finally, the review of data retention requirements included an analysis of existing records retention requirements in light of TBDF-related concerns.

In addition, there was a background study prepared for the Task Force which reviewed the trends in computer-communications technology. The objective of this study was to provide a concise review of the current state of computer-communications technology and to assess its likely short term directions, i.e. the next 5-10 years.

This report serves as both a summary of the more detailed and technical information found in the individual project reports and a synthesis of extensive discussions within government and with industry. As well, it is a review of relevant published materials in the overall context of sovereignty and transborder data flows.

The work relied heavily on the consultative process not only within government but also with industry. This consultation with industry included interviews with selected firms in order to collect data and obtain a more thorough understanding of the operations of industry, its use and management of information in relation to key TBDF factors. In addition, associations, as well as individual companies, were invited to submit briefs to the TBDF Task Force in order to identify specific concerns. Briefs have been submitted by the Canadian Independent Computer Services Association, the Canadian Association of Data Processing Services Organizations, the Canadian Business Equipment Manufacturers Association, Bell Canada and I.P. Sharp.

It is noted that some areas were not addressed in detail by the Working Group. More specifically these include confidentiality of data in general and privacy in particular; existing network information and transaction services (e.g., electronic fund transfers, credit and medical data); and new information and network services. These issues were omitted in the work program partly because of their close link to privacy considerations and partly because of a lack of resources available at this time. They are, however, important areas of concern and must be addressed in any further work on TBDF.

1.4 The Role of National Boundaries

Since the focus of the Task Force is on "transborder" aspects and impacts of data flow, it is useful to analyze briefly how the border functions in the context of current computer/communications technology. Traditionally, national boundaries which mark the territorial limits of the state, have also served as one of a set of locations at which sovereignty was exercised. Movements of goods and people were controlled at the frontier or at the limited number of locations where they first landed, i.e. ports, whether by sea or land and later by air.

National boundaries thus served not only to mark the territorial limits but also enabled countries to enforce national policies and practices with respect to the movement of physical goods and persons. Various international conventions, codes and agreements have been put into place in this respect.

Recent advances in the interconnection of the physical electronic networks, within a state and between states, have led to the development of electronic information networks whose functional boundaries are more often than not quite different than the national boundaries. Actually, electronic information networks act as, what geographers call, "functional economic areas". Relevant examples of functional economic areas would be the area from which a large city draws all its daily commuters or all the points served by an airline or trucking company. It is quite common for such functional economic areas to overlap several differing political jurisdictions. To date, the legal framework, domestic as well as international, has been able to adjust and adapt to new and different functional economic areas as they apply to the movement of persons or goods, i.e. tangibles; and the nation-state has maintained its ability to monitor and control such flows of goods if and when desired. Mechanisms used to maintain a national boundary include customs and immigration, landing rights, import or export restrictions, tariffs, etc. In the area of electronic communications, "physical boundaries" that do exist are basically those that have been imposed on the carriers and communication networks not on the flow or content. They are maintained through various international agreements and revenue sharing settlements. Examples are the telegram, telex and telecommunication networks.

The convergence of telecommunications with the computer in a time-shared network, coupled with the introduction of distance insensitive pricing, has led to the creation of numerous functional electronic information networks with boundaries of their own. For example, a computer time-sharing system that can be accessed from different parts of the world has its "boundaries" defined by the locations from which its users access the system. The result is that, for practical purposes, physical national boundaries have little or no relevance to an increasing number of computer/communication network users.

Direct extension of the mechanisms that have maintained national boundaries in the physical world to those of the electronic digitized world, therefore, may no longer be fully appropriate.

The need for an electronic boundary to assist in the maintenance of "cultural sovereignty", i.e. a distinctive national cultural identity, is becoming increasingly important to a number of countries which are either small or particularly susceptible to being engulfed by electronic cultural flows originating outside of their territory.

So far discussion of the "national boundary" and transborder data flow has taken place in the context of terrestial communication networks, the "electronic highways" of the communications world. In the context of non-terrestrial (satellite) transmissions the analogy of an "electronic ocean" seems more appropriate since a satellite exhibits more of the characteristics of a vessel in international waters than a truck on a highway.

In addition, satellite-based computer/communications introduce a unique dimension to the concept of sovereignty and national boundaries: they generate passive electronic information networks, i.e. the satellite footprint or spill-over. It may very well be that legally a satellite operates only on a domestic basis, however, in order to actively serve its target audience the satellite network inevitably and uncontrollably provides passive service to several countries. National boundaries, in functional terms and in relation to electronic data flows, are becoming increasingly difficult to maintain if the full benefits of advancing computer/ communication technologies are to be realized. Electronic boundaries, therefore, if they need to be created on sovereignty grounds may require policies and enforcement mechanisms of a different nature than those which currently apply to the movement of people and physical products.

In the Canadian context, the national boundary has two distinct characteristics with respect to transborder data flows, namely,

- the Canada-U.S. border which has almost disappeared due to the development of a functionally integrated "domestic" North-American communications network; and,
- the Canada-rest-of-the-world borders which are being maintained at present via Teleglobe.

The situation is further complicated because of questions raised as to the relevance of the national boundary concept to non-terrestial data flows including the automatic generation of passive electronic information areas (footprints) as a result of the use of satellites.

2. BROAD AREAS OF CONCERN

The issues of a TBDF-nature which have a relation to both the concept and exercise of sovereignty are many and diverse. In the course of the work, it became apparent that there were three broad areas of concern which required immediate attention. They are:

- concerns related to questions and problems of a jurisdictional, legal and regulatory nature raised by transborder data flows and the supporting technical infrastructure;
- concerns about the cultural impacts of transborder flows of data in the form of electronic information products and the formation of an electronic heritage; and,
- a general set of concerns about possible vulnerabilities associated with increased reliance by Canadian society on a computer/communications infrastructure and data flows intricately linked with those of other countries.

But before discussing these three general sets of concerns in detail, it would be useful to begin with a short discussion of the types of data which elicit or require greater concerns than others.

2.1 Classification of Data Flows 5/

Information or data are vital to the decision-making process and the delivery of services and goods in both the public and private sectors. The TBDF concern raised in this context is the problem of how the converging computer/communication revolution with its inherent disregard for national boundaries should be addressed with respect to the storage of data in Canada and the sharing of data outside of Canada. (Legal questions related to records retention and laws of evidence are addressed below). The development of a classification scheme for data flows would assist in removing some of the confusion which exists in discussions on TBDF due to the failure to distinguish between different types of data that flow. From both the perspectives of the public and private sectors, the following classification scheme for data in terms of TBDF might be useful in the analysis of the issues raised and the formulation of policies. In a simplified fashion, data could be classified as falling under one of the following four major categories:

Category A Data which should not be exported from Canada or to which foreign access should not be granted.

Category B Data which must be maintained in Canada but which may be exported, that is, copies may exist outside of Canada if certain conditions are met.

Category C Data which may be exported, i.e. need not necessarily exist in Canada, but which must remain accessible to Canadian

- government(s); and/or
- businesses; and/or
- individuals.

Category D Data which is exempt from TBDF policies.

Under Category A would fall such data which government and business have identified as being vital to their operations. For government this could be information which forms part of Cabinet decision-making process ranging from Cabinet minutes to budget data or information obtained in confidence from other countries.6/ There also exist provisions in various acts and regulations which impose restrictions on access to data, (e.g., Census), unless one is legally entitled to access to such data. In most cases, access to data falling under Category A is severely restricted within Canada itself at various levels of government and within and between government agencies themselves. Restriction on access, and therefore flows, are often time-sensitive, dissipating as the information ages.

In the private sector, industry does not wish that data protected by Canadian law or which can remain private under Canadian law become subject to access under foreign laws, regulations, investigative or legislative bodies. Information on market or pricing strategy, new product development, technical or production processes, mineral exploration test results, etc. are some examples of data which the private sector may label as Category A. Here also the value of much of this type of data has a strong time-sensitive element.

Under Category B would fall data of which the "primary or master" copy must remain in Canada but which could leave the country or be shared with foreign entities if certain conditions are met. In the public sector, there exist arrangements for the sharing of data related to such matters as defence, law enforcement, environmental and health matters, and with some countries on pensions and unemployment insurance. In the private sector, there is the exchange of proprietary technical and production data under licensing arrangements, the sharing of copies of data as well as transfer of data within multinationals. In the public sector, laws or regulations or instructions from the appropriate level of government provide the guidelines for the manner and form of such data sharing arrangements while in the private sector such arrangements are enforced through the operation of private commercial law.

Under Category C would fall such activities as the joint Canada-U.S. NORAD defense system where data gathered in Canada is transmitted to Colorado for processing and analysis but with access being ensured to the appropriate Canadian representatives. Similarly Canada participates in the development and maintenance of international data bases such as those related to atomic energy, agriculture, health, etc. In such cases, access is guaranteed to participants either through the receipt of copies or direct on-line access to the system in some foreign country. Two examples in private industry are the on-line system for airline reservations (SITA) and electronic fund transfers among banks (SWIFT). Individuals export data also usually in relation to the purchase of products, obtaining credit or participation in commercial ventures. In many cases, data falling in Category C are part of international activities of which the Canadian component forms only a minor

part. Industrial TBDF policies of encouraging indigenous data processing and maintenance through arbitrary restrictions on data outflows might be counterproductive in that one would need to take into account the value of participation in such international activities.

Data sharing and data access activities for data falling under both Categories B and C lend themselves to being covered by specific agreements, drawn up in accordance with general sets of principles or codes with subsections specifically addressing the differing natures of government, business or personal data. Such an approach would lessen the chance of the introduction of regulations or requirements of a "blunt instrument" nature and would identify specific problems which would be solved best by specific solutions or on case-by-case basis.

Following a more in-depth study of data storage and data sharing regulations practices in the public and private sector than was carried out for this report, it might be necessary to revise and refine this draft classification scheme.

2.2 Jurisdictional and Legal Issues 7/

To date, there has been very little analysis of the legal issues associated with transborder data flows. This probably is because it is premature to attempt such an analysis. The adequacy of existing law to deal with TBDF-related issues can be more appropriately assessed when a policy framework associated with this issue has been adopted.

However, a preliminary review of some of the legal aspects related to TBDF has been undertaken. The following specific items, discussed in great detail in the Project Report, "Legal Aspects of TBDF" are summarized below:

- domestic legal issues associated with computer use in the areas of: criminal law, existing legislative requirements concerning evidence and records, and patent and copyright;
- the potential international aspects of domestic legal issues;
- concepts such as "sovereignty and jurisdiction", and the rights of states under international law to control information beyond their borders, i.e. a question of extra-territoriality, or to control the flow of information from their territory.

2.2.1 Domestic Legal Issues Associated with Computer Use

(a) Criminal Law

There are two types of issues raised by computer/communications in the field of criminal law. The first is legal in the strict sense and concerns whether, as a matter of statutory interpretation, certain acts performed with or directed to computer hardware and software constitute offences within the meaning of existing provisions in the Criminal Code. The second issue is one of legal policy and concerns whether the criminal law should be amended to ensure that reprehensible conduct involving computers is proscribed or otherwise regulated.

The problems of computer crime can be divided into three distinct components. The first concerns the unauthorized acquisition or destruction of computer hardware and communication devices. These items are tangible and therefore already protected to some extent by the general provisions of the Criminal Code dealing with theft of property and mischief. In the case of software, however, it is questionable whether protection is accorded to the value of its actual physical content. The second aspect is the unauthorized acquisition alteration or destruction of data or software contained in a computer system. The third deals with the unauthorized use of computer services as measurable in time.

It has been clear since the decision of the Supreme Court of Canada in R. v. McLaughlin [1980] 2 S.C.R. 33 that a gap exists in the criminal law in Canada with respect to these latter two areas. This gap is related, in part, to the fact that under Canadian law property rights in information are not recognized. Thus, traditional notions such as theft and fraud cannot normally be applied to the unauthorized use or alteration of computer data. Recognizing this, the Crown in the McLaughlin case charged some University of Alberta students who had gained unauthorized access to the University's computer services and had copied data from personal files with theft of a telecommunication service under paragraph 287(1)(b) of the Criminal Code. The Supreme Court, however, held unanimously in that case that the University's computer was not a telecommunications facility but a computer centre. Thus, paragraph 287(1)(b) did not apply to the conduct in question and such conduct was found not to constitute a crime under the laws of Canada.

A key issue, thus, is now raised as to how the criminal law should deal with a person who obtains access to and uses computer facilities in an unauthorized way. This matter is being studied as part of the Theft and Fraud Project of the Criminal Law Review currently underway within the Department of Justice. It is expected the study will be completed within a year and that, within this time-frame, recommendations will be provided to Cabinet with respect to "computer crime" issues.

(b) Statutes Dealing with Records

(i) Laws of Evidence

There are a number of sections in the Criminal Code other than those relating to theft whose effectiveness in relation to new computer/communications technology is questionable. For example sections 300 and 324 dealing respectively with fraudulent destruction of documents of title and forgery, may become outmoded if the definition of "document" in the Criminal Code proves insufficient to deal with the increasing electronic storage of legally significant and financially important information.

There is some uncertainty in Canadian law about the admissibility of computer-produced records as evidence in judicial proceedings. In common law, the "Best Evidence Rule" has traditionally ensured that documentary evidence introduced in court is as accurate as possible by

the requirement that the original document be produced if available. Computerized generation and storage of information, however, has called into question what is an original document. Although it is generally agreed that the "Best Evidence Rule" remains a sound principle upon which to base the admissibility of documents, new techniques are radically changing what constitutes the best evidence actually available.

Most definitions of the term "record" included in provincial Evidence Acts do not specifically refer to computerized records. This is because the legislation was enacted at a time when computerized records were not an issue. While it is possible that many of the definitions of "record" in evidence statutes could be interpreted as encompassing such records, at the moment, whether, and the extent to which, they would be so interpreted, is unclear.

Reform of this area of the law to reduce the uncertainties involved has been suggested by the Uniform Law Conference in a Uniform Evidence Act drafted by the Conference. The term "record" is defined in clause 1 of the uniform code to mean:

"the whole or any part of any book, writing, other document, card, tape, photograph within the meaning of section 130 or other thing on, in or by means of which data or information is written, recorded, stored or reproduced".

At clause 130, "original" means, inter alia:

"in relation to stored or processed data or information, any printout or intelligible output shown to reflect accurately the data or information".

A "duplicate" includes:

"a reproduction of the original from the same impression as the original, or from the same matrix, ...or by other equivalent technique that accurately reproduces the original".

The drafters of the uniform code have understood that evidential guarantees against inaccuracies and fraud that have been obtained by insistence on the production of original documents will not be impaired by recognizing that advances in informatics have produced new forms of record-keeping. Although the form of recording and transmitting information may have changed, it is a natural development that the status of "original" be conferred on a computer printout. It is important to note, however, that the uniform code had not been adopted as law in any jurisdiction in Canada.

The current uncertainties with respect to the status of machine readable records as evidence in legal proceedings have undoubtedly led to some reluctance on the part of industry to convert totally to computer-based record keeping operations.8/ If changes are made to the law to

eliminate these uncertainties, the result may very well be an increase in transborder data flow.

(ii) Record Retention 9/

Another issue raised is the statutory interpretation to be given to the numerous provisions in federal and provincial statutes requiring that certain records be retained. In most cases, this requirement is imposed to ensure that information essential to government regulation and audit of business and other activities is available for scrutiny.

An important question is raised when such legislation requires that a record be kept at a specific place of business in Canada. Can compliance with such a statutory provision be achieved through retrieval by a computer terminal at the place of business, when the information is actually stored in a computer bank located elsewhere? It is clear that record retention requirements would be equally well served in many instances if machine readable copies of records were available. Thus, it is likely that statutes will be interpreted to accommodate these new forms of writing and record-keeping or, if this is not possible, that statutory amendments will be made.

A particular record-keeping issue which arises in relation to business information stored in computers is the impact this may have on the few statutes that are specifically designed, for reasons of sovereignty, to ensure that information does not leave the jurisdiction. One example is the Ontario Business Records Protection Act, R.S.O. 1980, ch. 56, which was enacted over 30 years ago specifically to prevent American anti-trust authorities from obtaining access to records of the Canadian business operations of Canadian pulp and paper companies. The relevant words of section 1 of this Act read:

> "No person shall, pursuant to or in a manner that would be consistent with compliance with any requirement, order, direction or subpoena of any legislative, administrative or judicial authority in any jurisdiction outside Ontario, take or cause to be sent or remove or cause to be removed from a point outside Ontario, any account, balance sheet, profit and loss statement or inventory of any résumé or digest thereof or any other record, statement, report, or material in any way relating to any business carried on in Ontario..."

In 1948, the Ontario legislature no doubt assumed that business records of Canadian companies would normally be kept in Canada. The purpose of the Act was not to impede the flow of business records outside the jurisdiction for business purposes, but to block compliance with foreign demands for business information located in Ontario. As the provision is drafted, the legislative purpose might be frustrated if a company kept machine-readable records in a computer in Ontario that could be accessed by a foreign authority from a terminal outside Ontario.

On the federal level, Bill C-41, The Foreign Proceedings and Judgments Act, would, if passed by Parliament, authorize the Attorney General of Canada under specific circumstances to prohibit the production of "documents" or the giving of information to or for the purpose of a foreign tribunal. The bill defines "document" as including:

> "any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microfilm, sound recording, video-tape, machine readable record, and any other documentary material, regardless of physical form or characteristics, and any copy or portion thereof";

This definition recognizes that the physical forms and characteristics of information are increasingly various and it provides a good example of how a potential problem posed by the new technology can be accommodated through appropriate statutory language. This bill has not yet been passed into law.

(c) Intellectual Property - Patent and Copyright

Another area where changes will have to be considered in domestic law to accommodate advances in computer technology is patent and copyright law. A patent right is a grant of some privilege or authority to prevent the infringement of a process, discovery or invention. A copyright is an intangible, incorporeal right granted by statute to the author of a work giving him the sole and exclusive right to make copies of his work and to publish and sell them. Whether or not computer programs are a proper subject of patent or copyright is an issue that has not been statutorily or judicially determined in Canada. These questions are now being examined in light of advances in the field of high technology. In particular, the issues raised have been incorporated into the revision of the law of copyright currently underway within the federal government.

2.2.2 Potential International Aspects of Domestic Legal Issues

Most of the domestic legal aspects of computer/communication technologies discussed above have international elements. Although the location of data processing and data storage may become technologically and functionally irrelevant, the transborder movement of data adds a relevant and complicating element in legal terms.

Public Law

Public law is the body of rules dealing with the state on its relation to individuals and their behavior. Generally, the law is interpreted as not having an extra-territorial application. However, under the principles of public international law, states are permitted to apply their laws to conduct outside their boundaries in certain circumstances.

These factors will have to be taken into account when dealing with the issue of computer crime in Canada. For instance, if a new offence of obtaining unauthorized access to a computer is created, will it make any difference if a terminal is located in Canada or the computer located elsewhere?

The law of patents and copyright also has an important international aspect because in practical terms, the effectiveness of the protection that can be accorded software or firmware under Canadian domestic law will depend in large measure on whether other states are prepared, as a matter of reciprocal treaty obligation, to recognize and protect such property rights within their respective jurisdictions. Some preliminary work is taking place at the international level aimed at developing new treaty obligations to fill the gaps and uncertainties that currently exist in the area of protecting computer software.

Private Law

Private law concerns individuals and their relation with each other (i.e. torts, contracts, etc.). The unparalleled geographical diffusion made possible by computer/communication technologies can also be expected to raise questions of private law, especially those such as choice of law analysis that arise when a set of facts with a foreign element is before a court. However, to date there is little information on actual legal problems that have been encountered in this area. Moreover, when encountered, there is no reason to believe that existing principles cannot be applied and, where necessary, adapted by the courts to deal with private law issues.

2.2.3 Sovereignty and Jurisdiction

Essentially, sovereignty in international law refers to the legal power to control national policies and to exercise jurisdiction over a determinate tract of territory and the inhabitants therein, without the consent or concurrence of any other state. Any restriction upon the exercise of this jurisdiction, not imposed upon a state by itself or by international law and deriving validity from an external source, constitutes a diminution of the state's sovereignty. It should be noted that practical constraints on what a state is legally entitled to do, do not amount to a diminution of sovereignty in a legal sense. In practical terms, this means that legally each state can enact laws that affect and bind real and personal property within its territory, all persons residing there and all contracts made and acts done within it. Conversely, a state cannot, generally speaking, through its laws directly affect or bind property outside its territory or bind persons not resident there. An exception to this latter principle is that each state has the right to bind its own subjects by it laws, wherever these persons may be although enforcement of that right may be difficult. In addition, international law recognizes a number of other principles upon which states may rely to justify an assertion of jurisdiction beyond their borders.

With respect to the ability of a state to enact laws of binding effect outside its territorial jurisdiction, it is therefore important to recognize that a state does not have the power to enforce its laws beyond its territory. It does however occur that a state in demanding that its nationals (natural or legal persons) to comply with certain domestic laws or manner under regulation is in effect enforcing the practical application of its laws outside its territory.

One consequence of electronically communicated transborder data flows is that even if Canadian laws could properly apply to data stored outside of Canada such data are outside of Canada's physical boudaries and hence outside the enforcement jurisdiction of Canadian law. This has implications for the rights of privacy granted under Canadian law to its citzens when personal information about Canadians is stored outside Canada even though such privacy laws applicable to the private sector are at present virtually non-existent. It also has implications for maintaining the confidentiality of information, deemed to be confidential under Canadian law, where the information leaves the jurisdiction. Other implications that have been noted by the various recent studies into, and articles written about, this issue are the potential frustration both of government policies that require the production of information for decision-making purposes and Canadian court orders for the production of certain records, where this information and these records are located outside Canada's territorial jurisdiction.

It is to be further noted that even if Canada could justify an attempt to control Canadian data stored abroad based on, for example, the nationality of the entity controlling the data, the applicable Canadian law may well conflict with the regulatory regime governing the data that applies in the state in which the data are located. As a practical matter, in such circumstances, Canadian law and policy would probably have to cede to the jurisdiction of the state where the data are located.

Conversely, it is clear that Canada has full and complete jurisdiction to apply its laws to data originating in another country that are stored here. In short, transborder data flows do not interfere with the ability of valid Canadian law to regulate the manner in which data is stored, processed and handled in this country. In the interests of all countries, therefore, international agreements on extraterritorial questions with respect to data whether bilateral or multilateral, may be necessary in the future.

3. CULTURAL ISSUES 10/

In its early days, data processing and telecommunications applications related primarily to "number crunching", scientific analysis and business and financial data. Cultural effects were practically non-existent. Advances in technology, reductions in costs and wide-spread use of computer communications, at all levels of society, have created definite cultural impacts. It is, therefore, not surprising that transborder data flows have raised concerns about the impact on "cultural sovereignty". In the context of this Report cultural sovereignty is defined as the assurance of a viable indigeous cultural expression through a variety of communications and computing media.11/ "Cultural sovereignty" does not imply isolation or protection from international cultural forces, i.e. data flows from abroad. Instead the term should be interpreted as a national commitment to feed and nourish the country's cultural heritage based on a positive commitment to build up one's own culture rather than a negative or restrictive approach.

In both a technical and wider sense, cultural concerns raised by transborder data flows range from broadcasting to video and audio recording as well as any type of electronic (digitized) products including video games. The initial focus here is on those cultural impacts which are new and related directly to transborder data flows. In particular, attention is focused on the electronic cultural heritage, i.e. machinereadable data files and electronic cultural products, i.e. public on-line information retrieval services.

There are cultural dimensions to Canada's external account. The cultural sector generally presents a picture of massive imports equivalent to several times the amount of exports, the major trading partner being the U.S. Also the imports have dominated the Canadian national market in the cultural sectors. For example, in the book industry of $600 Million total market revenues in 1977, import sales totaled approximately $432 Million. In terms of ownership of companies, foreign owned operations in Canada have traditionally been seen to have several advantages over Canadian-owned. They generally are _____ to have more efficient management and order-processing capabilities; they have access to the parent's company's expertise and familiarity with marketing techniques; they generally have easier access to development capital for expansion; and they have access to the parent's files on which "Canadian" adaptation can be accomplished at minimal cost. Given these advantages, foreign branch plants have been able to move in and capture a major share of the Canadian market.

The educational and cultural impact of these trends in the cultural sector emerges when, as has been the case, the Canadian perspective of the world and of itself is transmitted through imported products. The analogy to machine-readable data is self-evident, especially when one considers the potential development in the area of electronic publishing and information retrieval.

The government has established a wide range of programs to improve the balance in the other cultural sectors. In the area of machine-readable data steps can be taken prior to the emergence of similar problems.

Current government policies and regulations designed to protect, ensure the survival of, or stimulate, Canadian cultural products and heritage are technology bound. That is, they differentiate between and focus upon either specific physical products (e.g., books, films, periodicals, etc.) or particular modes of transmission (e.g., broadcasting, cable, telephone). Advances in the convergence of computer/communications technologies, coupled with the trend to using these technologies to produce these products, are rapidly making this traditional approach obsolete. All these products will soon have a digitized counterpart. The two immediate cultural sovereignty concerns most closely and directly linked to transborder data flows are those pertaining to cultural products and heritage which exist in electronic (digitized) mode only. However, it should be noted that concerns, problems, principles, arguments and solutions developed on the basis of these two arbitrarily narrow cultural aspects could be equally applicable to other future digitized cultural forms.

3.1 Towards a Canadian Electronic Cultural Heritage 12/

As new technologies are being increasingly applied, the record of the development of various facets of Canadian society is now often available in electronic machine-readable form only.13/ Because of their inherent technological properties, machine-readable data files of archival value might well suffer from benign neglect on the part of the government and other interested parties. It is not possible to place computer tapes in dormant storage for a number of years before giving them adequate conservation treatment as has been the case with paper, hard-copy or physical cultural properties; these traditionally have continued to exist for some time, unless destroyed by design or accident. The electronic cultural heritage on the other hand will have to be consciously created through its extraction from the daily activities of society since the nature of computer operations is such that data, no longer needed for operational or legal purposes, are automatically purged.

The lack of a publicly-available electronic cultural heritage in a format which will make it easy to use in Canadian educational institutions, and for general research purposes, not only creates an increasingly serious deficiency in Canadian ability "to know ourselves" but also creates a tendency to import machine-readable data files from other countries to fill the void. On an ongoing basis, these data files, however, are needed for training in quantitative methodology especially in the social sciences. The apparent paucity of machine-readable data files containing Canadian data, therefore, directly results in a growing knowledge of cultures other than our own.14/ There is a parallel here with the proliferation of foreign textbooks in Canadian schools. The difference, however, rests in the fact that in the area of electronic data sets there is, at least for a brief period of time, an opportunity to fill this void with Canadian material and thus avoid a major problem, whereas in the area of text books we are in a position of attempting to minimize what has long ago become a major, perhaps insurmountable, problem.

Since the transborder data flow question here is basically one of importation due to either lack of indigenous supply of machine-readable data sets or lack of knowledge of availability of an indigenous supply, the immediate

creation of an inventory of domestic machine-readable data files, and an active program aimed at rapidly expanding and publicising these, is required.

There is one further consideration. Machine-readable data files, while having a certain similarity to other cultural products, are also unique. One may need mechanical assistance to view a negative or view a film and one needs a computer to read a machine-readable data file. However, in order to read a machine-readable data file, the file itself must be "readable" and adequate documentation must also be available. It is not enough to simply have numerous machine-readable data files documenting a multitude of aspects of the development of Canadian society if these are not in a condition which would allow them to be easily used by Canadians. Means must be found to create a practical and useful core stock of machine-readable data sets, that meet Canadian requirements, which are publicly available and which are actively disseminated for use in the study of subjects having a high degree of cultural content. Only in this way can we ensure that the current dependency on imports of this type of data flow will diminish.

One further aspect of the development of Canada's electronic cultural heritage impacts very directly on cultural viability and transborder data flows. In the past, private sector entities, even if foreign-owned, tended to keep books of account and other company paper records long after they were needed for operational and legal purposes. As a result, the Canadian cultural heritage traditionally has been enriched by private archives or the donation of these private archival materials to public archives, often 50 to 100 years after their creation. This tradition may, in the absence of some action on the part of industry and/or government, disappear.15/ One impact of the use of computers is therefore that it raises the question of whether data will be kept at all, as obsolete data is automatically purged, i.e. the goal of information resource management is to maintain only data that is timely, relevant and up-to-date for decision-making purposes or because of legal or regulatory requirements. To the degree that records of the activities of the private sector (whether in public or private archives) form part of Canada's cultural heritage, the question of whether or not there will be an archival heritage in electronic form is real.

The sovereignty impact of this development relates to the question of where the data is stored. Current technology allows for the collection, storage and maintenance of such Canadian information, in centralized data banks, conceivably located in any number of countries outside Canada. While access to these Canadian data by Canadians would be via remote terminal facilities, one result could be that, no local records on some aspects of Canadian society may exist 100 years from now within Canada. Further, from a Canadian perspective there may be a different set of priorities than those of the operator of the data base as to which data, no longer needed for operational purposes, warrants preservation as part of the electronic archival heritage. It should be noted that this is part of an overall sovereignty concern of considerable importance and has major transborder data flow connotations insofar as organizations operating in several countries centralize data storage and maintenance activities outside of Canada without any copy being kept in Canada.

Insofar as the study of a people and detailed knowledge about them has a cultural aspect the location of personal data banks abroad, in addition to privacy concerns, raises specific cultural heritage questions. For example, if an international union were to automate its records-keeping activity and maintain its data bases and archives at its foreign headquarters, future Canadians studying the labour history of a Canadian town or a certain industrial activity would be forced to go outside Canada and request the permission of non- Canadians to access the necessary Canadian information, that is if the data still exist or has been tagged as Canadian when merged with a larger data base.16/ This is a cultural aspect of transborder data flows quite unique and separate from any privacy considerations. In the case of hard-copy records, this eventuality is covered by the Cultural Import and Export Properties Act which is intended to provide a means for maintaining the physical cultural heritage of Canada by restricting the out flow of such properties. No "electronic" equivalent of this Act exists.

3.2 Electronic Cultural Products 17/

The government has always been actively involved in the support and development of Canadian cultural industries through a variety of programs, legislation, regulations and fiscal incentives. In this respect the cultural implications associated with on-line data base activities and the flow of information warrant special attention.

It is only during the past five years that on-line data base activities have moved from an experimental stage to a full fledged industry on the verge of entering the mass consumer market. The growth in the size and number of on-line data bases offered publicly for sale has been very rapid and shows no sign of abating. Recent advances in software techniques coupled with decreasing computer and telecommunication costs suggest that this industry will continue to grow at a very rapid rate in the years ahead.18/

While it may prove difficult to measure the specific cultural content of on-line data bases, there can be no denial of their cultural impact.19/ Figures available from a study of the public on-line information retrieval industry indicate a very strong dependency on foreign content. For example, less than 40% of the reference data bases currently being accessed by Canadians are of Canadian origin, a level of dependence on imports which is not unlike that for other cultural products.20/ However, if one measures Canadian content in terms of numbers of citations or references in Canadian data bases versus the other data bases being accessed, the "Canadian content" is only 3½%.21/ It should be noted that Canada accounts for approximately 5% of the world's research activity.

It also seems that out of each $10. spent by post-secondary Canadian educational institutions on public on-line retrieval services, only $1. goes to Canadian owned and operated data bases.22/ It would seem likely that customer preferences established in college and university are likely to be continued later in life. Even in the federal government roughly 66% of each dollar spent on on-line information retrieval goes to foreign services.23/ Only in areas where the data in source data bases are unique to Canada, such as in the legal area or electronic newspapers such as InfoGlobe or Newstex, does there seem to be a reasonable level of Canadian activity. To the

degree that machine-readable data files provide the feedstock for the information retrieval industry, any activity which would encourage or expand the electronic cultural heritage will also assist the creation of a stronger Canadian content in this cultural industry and may thus lessen the import aspect of transborder data flow and, perhaps, even lead to some exports.

Currently, no policy or analytic framework nor statistical base is in place which directly addresses the problems enunciated above. Available data indicate a strong off-shore dependency in on-line services and concurrently, both a relative and absolute weak indigeneous capability in the production of data. A viable Canadian culture depends on the capability both to withstand, not merely restrict or restrain foreign cultural competition at home and to compete effectively abroad. The success of policies designed to maintain and promote a vibrant Canadian culture, therefore, will depend not on a predominantly protective defense of home turf but on an outward, competitive cultural industry thrust that takes full advantage of the burgeoning continental and global information, entertainment and computing markets. The principles and arguments developed with regard to on-line information retrieval services are essentially applicable to other future digitized cultural forms as well.

Apart from the immediate need to fill information statistical gaps in this area, there are a number of measures which warrant consideration as elements in the development of national information policies:

- the role of the private sector in the provision of data base creation and on-line information retrieval services for government;
- the extension of current government EDP "make or buy" procurement policies to include data base creation and information retrieval services;
- a mechanism that will make data files created with public funds available to private industry for information packaging and distribution;
- programs designed to give appropriate incentives to Canadian data base creation and information retrieval services;
- programs designed to encourage and assist entry of Canadian private and public sector information services into international as well as national markets;
- the development of on-going mechanisms to make Canadians aware of existing data files and data bases and to ensure the widest possible access to these.

4. VULNERABILITY ISSUES 24/

4.1 Introduction

The subject of vulnerability issues is complex. It extends beyond the technical aspects of computer/communications security by virtue of their widespread impact on society. Detailed studies of vulnerabilities related to TBDF in the context of a rapidly evolving and changing technology do not exist. While much has been written on the question of the vulnerability of the "computerized or wired society", transborder data flows and other issues arising from the impact of advancing and converging computer/communications technologies have not been specifically addressed nor has the debate as such advanced substantially. A few countries have begun initial reviews of these issues but only Sweden has taken practical and concrete steps to address them in an intergrated and ongoing manner and under a clearly defined responsibility centre.

No study has been carried out on the vulnerabilities of Canadian society although a number of vulnerability issues have been noted, (e.g., the Report of the Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty (Clyne Report), 1979 or The Information Revolution and Its Implications for Canada, 1980). It is clear, however, that the transborder question does, and will exacerbate any domestic vulnerabilities flowing from rapid computerization.

A critical factor is that the increasing ease with which one can transmit data electronically, physically and economically, and link computers between countries, lessens the degree to which territorial national boundaries have a functional relevance to users of such computer/communication systems. The importance of this finding is that it will become increasingly difficult in a number of areas to distinguish between vulnerability issues of a domestic and transborder nature. Furthermore, new or increased vulnerabilities arising in other countries can impact almost immediately on Canadian computer/communication system users and society.25/

Even when specific vulnerabilites can be identified the question arises as to who will be responsible for dealing with or minimizing these vulnerabilities. Normally, reducing the vulnerability of a computer system is the responsibility of the organization which operates the system. In the case of shared international networks or data, in a true distributed data base system spanning several countries, there is considerable uncertainty as to who in an organization (public or private sector) will be accountable for minimizing disruptions and ensuring data integrity. 26/ There are no domestic or internationally accepted rules or practices - in fact, there are no rules.

New technologies can be used to reduce risk by being designed to operate more reliably than the mechanism they replace or through the introduction of additional systems redundancy, i.e. through the use of alternate data transmission routes, distributed data bases, back-up computers, etc. As society becomes more dependent on the reliable functioning of a growing number of major integrated systems, it will have to balance the vulnerabilities it may

encounter against the benefits it may receive: an assessment which by definition must involve more than just the technical or economic aspects. Failure rates may be low but the potential losses in financial and social cost could be very high should disruptions or failures occur.

There is a rapidly growing need to create awareness, understanding and workable mechanisms to determine the tradeoff between the many positive aspects of computer/communication technologies and the new vulnerabilities they introduce. There is a further need to minimize, in all instances, the vulnerabilities that society chooses to accept. The transborder nature of these systems greatly compounds the problem of vulnerability.

4.2 Computer Security 27/

The first set of vulnerabiity concerns focuses on the reliability of computer systems and the ability to protect systems, data and services from accidental and deliberate threats to confidentiality, integrity or availability. Security is largely a negative attribute. It is difficult to demonstrate its presence. While much emphasis in the past has been placed on the physical security of computer installations, in our context the emphasis is on the system itself and security is really the prevention of "harm" to the system and the data it carries such as:

- disruption to, or denial of, the use of computer systems and their contents;
- unauthorized access to, or release of, information i.e., breaches of confidentiality and privacy;
- unauthorized modification, manipulation of the content;
- destruction of data or software programs; and
- accidental error.

In the context of transborder data flows, stand-alone computer installations, i.e. those that do not allow remote access, can, by definition, not be accessed from outside Canada and thus do not present a transborder concern.

One of the major problems related to computer security is a general lack of awareness of the vulnerability of most computer systems to misuse. This is exacerbated, in part, by the widespread belief that changing and advancing technology will make the problem go away as well as a reluctance to incur the costs required to make a system more secure.28/

A number of recent developments are creating new or increased risks in breaches of security. They are:

- the trend to linking a large number of computer systems together to be used for diverse applications by many persons at different locations. This poses system design and management security problems that are orders of magnitude larger than found in the design of previous generations of information systems;

- the growing shift of user demand from batch over-the-counter data processing to remote and interactive computing services. In 1965 batch held a 9:1 ratio over interactive processing. By 1985, the ratio is expected to be reversed;
- the rapidly increasing quantity of computerized data stored and transmitted over communication networks, as well as the increased capability of the networks to carry greater volumes at higher speeds and lower per unit costs, (e.g., packet switching);
- the increasing trend to "user-friendly" computer systems without a corresponding review of the adequacy of security measures;
- the introduction and rapid spread of low-cost microcomputers (personal and business) which by the mid - 1980s could well number over 5 million in North America, alone. Already more than 10% of these have communication capabilities and this is expected to increase;
- the increasingly large number of businesses using, and therefore being able to access computers; and,
- the increase in the number of students and others acquiring computer know-how.

However, one major factor is emerging as fundamental: there is no general agreement on what constitutes computer crime or abuse. There are presently no penal consequences attached to fraudulent use or abuse of computer systems and data. For example, the concept of theft of computer time is not universally accepted, and to many individuals the breaking of computer/communication security systems represents a challenge not to be ignored. No reliable data on computer crime exist in large part because of lack of definition and legal recognition. In addition, no distinction is made between the computer as an instrument in executing a criminal act, i.e. like using a pen to forge a cheque, and the computer or its data as an object of abuse. It is in the latter area that proposals have been made to amend the Criminal Code such as to make the fraudulent or unauthorized use of a computer or any part of the related access network right back to the terminal an offense. As well, the proposals would make it an act of mischief for persons without authorization to damage, destroy, or alter data or information stored in a computer.

Such amendments to the Criminal Code for "computer crime or abuse", if enacted, will reduce domestic vulnerabilities. They will not, in the absence of clear and specific agreements with other countries, from which unauthorized access and use of computer systems may take place, reduce overall vulnerability. In fact, as the communication networks of countries increasingly are linked, the potential vulnerability of each increases in relation to the increase in the number of possible remote access points and computer-literate individuals.29/

In summary, the trend is one of increasing national and individual vulnerability in the computer/communications world. An adequate policy framework does not exist which recognizes these vulnerabilities and therefore seeks to control if not eliminate its possible harmful effects.30/ It is imperative that Canada commence work on such a framework especially since public concern and anxiety is on the increase.

4.3 Communication Networks and Security of Data Flows

Many network vulnerability issues can be considered simple extensions of those in any multi-use, resource sharing local computer network. As the communication networks increasingly rely on sophisticated computers for switching and routing of data traffic, these computers, like any communicating computers, are susceptable to attack. Therefore, computer system and data communication system security must be viewed as a common issue. This is especially true in the context of transborder data flow concerns.

With respect to vulnerability of the data flows or data storage, encryption seems to provide one answer. The past decade has seen an enormous advance in the development of more rugged and less costly encryption methods. The use of encryption in electronic data flows raises a number of specific data flow issues due to potential conflicts in national policies and regulations.31/ The possibility that some countries could prohibit the use of encryption or require registration of encryption codes, thereby allowing for the monitoring of information transmitted via international networks, has caused anxiety for industry. This is true especially where the confidentiality of client information is essential, (e.g., banking, insurance), or where the information transmitted has a high value, (e.g., high technology, "know-how", resource data).

For some countries (e.g., in Europe), the fact that they have to rely heavily on other countries for routing of their data transmissions abroad raises vulnerability concerns. Its geographic position and advanced telecommunication capabilities makes Canada less vulnerable to, or dependent on, terrestrial transborder data flow via third countries. Canada has direct links both terrestrial and nonterrestrial with those countries accounting for the vast majority of its data flows.

4.4 Use of Satellites

Satellite-based data communication networks offer reduced costs and vastly increased capacity for data flows. Such networks not only form an alternative to terrestrial-based networks but also open up many new transborder data flow opportunities. As a result, the concerns discussed in this report will be heightened in the context of satellite transmissions.

In addition, concerns have been raised about the possible vulnerabilities due to remote sensing by satellite. The vulnerability is perceived (by some countries) as the "siphoning off or theft" of information on a country's resources and possible state of wealth. It is feared that vulnerabilities are introduced when one country has a marked technological advantage of access to such superior data collection, transmission and processing, this being easily translatable into a substantial strategic or economic advantage, i.e. advanced or sole knowledge about mineral deposits or potential future agricultural crop yields.

While remote sensing remains a vulnerability concern in the transborder data flow debate, Canada has minimized possible vulnerabilities by creating a viable and technologically advanced indigeneous capability. At the same

time, the policies currently followed by Canada in its use and sharing of remote sensing data with affected third party countries should help to meet many concerns in this respect.32/

Finally, the use of satellites to assist in locating airplanes or ships in distress is just one of the many ways in which they can be used to reduce vulnerabilities.

4.5 External Threats

As the use of computer/communication systems becomes more pervasive and more critical to economic and military functions, a country becomes more vulnerable to other factors such as terrorist attacks on its computer/ communication systems, attacks launched via transborder telecommunication facilities. Also since computer systems and the data they contain represent increasingly dense concentrations of value, they naturally become targets to both domestic and international terrorist groups, organized crime and individuals.

Another vulnerability arising from external threats is that in time of war one must count on decreased use of computer/communications. The Swedish study on vulnerabilities noted that emergency planning for computer/ communication systems was not what it should be. In Canada, Emergency Planning Canada finds it not prudent to rely on computer/communication in times of nuclear war. For one, vital national information systems that need protection or contingency arrangements whether in war or peace have not been sufficiently studied. Although contingency planning, as such, is not a transborder problem, serious considerations do arise if the contingency plans include the provision of computing centres or the storage of essential records (data) in another country, to which access may be disrupted.

Finally, the phenomon of electromagnetic pulse and its potential to severely disrupt, if not disable, computer/communication networks, as well as all micro-electronic-based products and services, has received much attention. Protection against EMP is more a domestic vulnerability question even though EMP will probably continue to surface in the context of transborder data flow questions and should receive adequate study.33/

4.6 Personnel

Other Task Force reports deal with the question of skilled manpower supply, skill dislocation and possible employment/unemployment due to advancing technologies, in general, and transborder data flows in particular.

- In the context of vulnerability issues, the question of remote on-line diagnostic and repair service centres represents a new set of vulnerability concerns for Canada since so far most of these centres are located offshore, i.e. in the U.S. Whether or not the introduction of remote on-line diagnostics and repair services reduce vulnerability of computer systems by offering timely, complete and reliable (often 24 hour) trouble-shooting and repair services as opposed to increasing offshore dependencies on repair and maintenance expertise and possible compromise of data confidentiality, is a

question which could not be addressed by the Working Group, at this time, but is one which warrants serious attention both from an economic and minimum self-sufficiency point of view.34/

One new set of concerns regarding personnel and transborder data flows has arisen in Europe as multinationals are closing plant use mainly to weak economic conditions. The proposals, known as the Vredeling Proposal, would require a multinational company to release sensitive data on its operations in other countries to workers in that country where it proposes to lay off significant number of workers and/or close a plant, i.e. a forced transborder data flow.35/

4.7 Questions of Concentration

The question of increased vulnerabilities due to concentration, either functionally or geographically, arose in the 1970s and in the transborder data flow debate. In countries where data storage and processing activity has tended to be concentrated in a few locations and computer utilization was predominantly via large mainframe, it was felt that such concentration of computers and data greatly increased vulnerabilities. In the 1960s and 1970s computer systems in Canada were concentrated mainly in Montreal, Ottawa and Toronto. Currently, geographical concentrations of computers are found in the provincial capitals as well as Saskatoon, London, Calgary, Kitchener-Waterloo to name a few. Thus vulnerabilities, in this sense, have lessened considerably. Also, the trend towards using stand-alone minicomputers and distributed data procesing is further mitigating vulnerabilities due to geographical concentrations. Nevertheless, its vast geography continues to make Canada more dependent on safe and secure communications than smaller countries and thus more vulnerable to potential disruption.

Closely related to vulnerability questions related to geographical and functional concentrations of computer systems are concerns about concentrations of data. During the past few years, both the public and the private sectors have developed sensitive functionally concentrated systems in such areas as personal data banks, banking, airline reservation, insurance services, corporate management systems, etc. Not being a unitary state, like many in Europe, jurisdiction is shared in Canada. This has the effect of dispersal of government data banks both geographically and in extensiveness and detail of contents. As such Canadian vulnerabilities in this area tend to be less severe than those of their European counterparts. Besides most of these vulnerabilities are of a domestic nature.

4.8 Role of Information and Vital National Information Systems

A clearer and better understanding of the role of data or information is vital to coping with the information revolution as is the identification of "national information systems" which serve as the main underpinnings of the information society. Their disruption and consequent loss of data integrity would harm national interests. Insofar as these systems can be subject to remote attack, the element of transborder vulnerability is introduced. It was not possible within the resources of the Working Group to identify such vital national information systems, but it is considered important that this

be done especially the establishment of criteria for such systems. It may be useful to note that a study recently released by the U.S. Office of Technology Assessment on Computer-Based National Information Systems used the following criteria in defining vital "national information systems".

- substantially national in geographic scope,
- substantial national interest involved,
- organized by government or private organizations or groups to collect, store, manipulate, and disseminate information about persons or institutions; and,
- based in some significant manner on computers and related information and communication technology.

U.S. examples include FEDWIRE (an electronic funds transfer network operated by the Federal Reserve System), nation-wide computer-based credit card and check authorization services (e.g., VISA, American Express, Mastercard, Telecheck, Telecredit), nation-wide electronic mail services operated by several private firms and the U.S. Postal Service, computerized air traffic control systems, airline reservation systems of major air carriers (e.g., United, TWA, American), the computerized automatic quotation system for obtaining over-the-counter stock prices operated by the National Association of Securities Dealers, interconnected networks of personal computers such as MicroNet or the Source, etc.

In Canada, no such vital systems have been comprehensively identified nor their susceptability to domestic and remote disruption analyzed.36/ This must be done in order to discern whether concerns are justified and if so what adequate protective mechanisms need to be put in place.

With respect to data themselves, a well-established program exists in government for reducing the vulnerability of unauthorized or accidental disclosure of classified data. Likewise programs do exist for vital records although their application to machine-readable records is undergoing further development. What is not being addressed is the question of what is meant by "sensitive" non-classified data. The enactment of access to information and privacy legislation by different levels of government will assist in identifying "sensitive" data in the public sector. However, much of the transborder debate over sensitive data focuses on the non-public sector, and this has not been addressed, as yet, in any focused manner.

Apart from providing a summary review of vulnerability questions and the transborder context, the debate or clarification cannot progress much further until an acceptable working definition is given to "vital national information systems" and the question of "sensitive" but non-classified information is addressed in the private as well as the public sector.

5. OTHER CONSIDERATIONS

As stated in the introduction one of the project reports examined in some detail, the question of data retention and data storage.37/ From this report spring some major considerations, namely classification of data flows and location of data storage in the context of TBDF. The question of classification has already been dealt with.

3.1 Data Storage

Both government and business need to retain data or have access to data. On the side of the federal government, it requires business and individuals to submit data or retain data in order to ensure compliance with its laws and regulations. In the context of TBDF, the question is raised as to whether these data need be retained in Canada, i.e. does the existence of "Canadian" data outside of Canada affect the ability of the government to maintain "law and order", ensure compliance with financial, health and safety, environmental, tax, etc. legislation and regulations?

Until the advent of computer/communications, records were usually stored where they were created or used. Copies or summaries of records may have been sent and kept elsewhere but the question of the location of where data were to be stored did not really arise until the advent of inter-active multi-user computer/communications systems. The introduction of such systems with their remote input and retrieval of data made the question of where the data is to be stored distinct reality and the question of location of data storage a TBDF concern.

One important reason why businesses (and individuals) maintain data is because the government requires them to do so. The need for a general review of these records retention requirements or "paperburden" has long been recognized and has during the last few years been a major focus of the regulatory reform effort of the government. The federal government's efforts at regulatory reform are currently focused on reviewing the need for these records retention requirements and determining how long businesses are required to keep records. Of the 76 laws and 111 regulations which require business to retain certain records less than half stated specifically how long these records or data are to be maintained.38/ Only a few regulations mention that the record must be kept at a specific place in Canada. Most do not and until recently the question of where records had to be kept was a moot point as they were normally kept in hard-copy form and on-site. Many of the requirements to maintain data seem to place the emphasis on an ability to "produce required information during normal business hours". This requirement is often stated in the form of "one must keep records" or "books of account". If the regulation is simply one of "being able to produce", the obligation might be met by the ability to call up from a computer via a remote terminal, the required data, making a print copy if so desired.

The advent of computer/communications technology offering a more efficient and cost-effective means for storing data coupled with proposed changes in the legislation on laws of evidence will increase the need to review records

storage requirements not only as to what data must be maintained, how long, but also how, (e.g., machine readable), and where. Should domestic law and regulations allow for such records to be kept in machine-readable form, it will be necessary to specify whether or not the data in question or a copy need be kept in Canada in order to ensure that Canadian laws and regulations can be enforced. Consequently from the perspective of TBDF concerns, the inclusion of a review of how and where records are to be stored or retained in the general review of records retention requirements currently taking place under the regulatory reform program warrants serious consideration.

Not only does government require business to maintain specific types of records, it also needs to have access to business records in general in order to be able to enforce specific laws and regulations pertaining to the conduct of business. The question of the government's right of access to data relating to the affairs or property of Canadians extending beyond national boundaries received attention as early as 1977 when amendments to the combines Investigation Act were proposed.39/ The recently tabled proposed draft of a new Bankruptcy Act would give the Superintendent the power to require the production of Canadian data regardless of the location of the data banks of the business in question.40/ In other words, the advent of the use of computerized record-keeping systems by business for reasons of cost-effectiveness and efficiency has brought to the fore the question of where records are to be stored especially where such systems are international in nature, i.e. involve more than one national jurisdiction.

On the one hand, the government wishes to ensure that its right of access to Canadian data is not frustrated by the new technologies. On the other hand, there are also a few statutes that are specifically designed for reasons of sovereignty to ensure that Canadian data does not leave Canada. The purpose of such legislation is not to impede or restrict the flows of business data outside of Canadian jurisdiction. Instead, the purpose is to protect Canadian businesses from having to comply with foreign demands for business data. For example, the proposed Protection in Respect to Foreign Procedings and Judgements Act (Bill C-41) would under specific circumstances prohibit the production of "documents" or the submitting of information to or for the purposes of a foreign tribunal. While Bill C-41 would be effective against the forced production of hard-copy documents, it is not quite clear how it would apply in situations where those in other jurisdictions have on-line access to Canadian computerized record keeping systems.41/

FOOTNOTES

1. The terms of reference of the Interdepartmental Task Force on Transborder Data Flows are:

   - to provide the interdepartmental mechanism for joint planning and co-ordination of federal policies and programs relating to activities affected by transborder data flows, in particular the sovereignty and economic implications, and to advise the government on these matters through the Minister of Communications;

   - to discuss and exchange information on the research programs and projects, active or planned within the government and other countries and their effect on Canada;

   - to undertake joint interdepartmental research efforts designed to establish the necessary factual and conceptual basis for the development of relevant recommendations; and,

   - to develop the necessary processes or mechanisms to ensure an adequate data base on various aspects of transborder data flow and to recommend additional research as required.

2. Further discussion on different aspects of sovereignty are found below in this Report under Chapter II.B.3, the Report on Legal Aspects, pp. 35-57, (hereafter cited as Legal Report) and the Report on Cultural Sovereignty and Transborder Data Flows: On-Line Public Information Retrieval Services and the Canadian Electronic Cultural Heritage, pp. 5-7 (hereafter cited as Cultural Report) and the Report on Vulnerability Issues (hereafter cited as Vulnerability Report).

3. For example, the Dalton School incident and others as described in the Vulnerability Report.

4. This is a joint project with the Economic Aspects Working Group.

5. For a more detailed discussion consult the Report on Data Retention and Data Storage (hereafter cited as Data Report).

6. The question of flow of data is closely related to access to data and security of data since flows of data can only take place if the data in question can be communicated to others. There have been some cases where domestic restrictions on access to data have been construed as a transborder data flow restrictions, i.e. the Burroughs complaint against the Canadian Employment Insurance Commission. (For details see the Task Force's Data Report). In this context, freedom of information legislation enacted several years ago in the U.S., has led to both government and industry to be more specific as to what kinds of data need to be kept confidential thus severely restricting data sharing and data flows. One can expect that recently enacted federal access to information and protection of privacy legislation will lead both government and industry to define more precisely what data is confidential and which is not.

7. Since Chapter II.B is essentially a summary of the major elements of the Legal Report, the reader is advised to consult the Legal Report for a fuller and more precise discussion of legal questions.

8. Corporate secretaries and records managers in industry have pleaded for a long time to allow for the admissibility of both microfilm as well as computer-produced records in legal proceedings on an "as and when" required basis. They have and continue to make the point that the full cost-savings made possible by the use of the new technologies for record-keeping purposes will not be realized if duplicate sets of records in hard-copy form must also be maintained. The American Records Management Association (Canadian Chapter), the Canadian Micrographic Society and the Financial Executives Institute are some of the industry associations who have made such requests already for a number of years. See also the Task Force's Data Report.

9. For a survey of Federal government legislation see Records Retention Requirements for Business, a 1980 publication of the Government of Canada Office for the Reduction Paperburden. The work of this Office is being continued by the Office of the Coordinator, Regulatory Reform, Treasury Board Canada and the Advocacy Office, Small Business Secretariat, Industry, Trade and Commerce. For a more detailed discussion involving various practical aspects see the Data Report and also Section E.1 below on Data Storage.

10. Chapter 2.3 is both a summary of the Cultural Report and certain sections of the Report on Public On-Line Retrieval Services (hereafter cited as On-Line Report). Readers are advised to consult these reports for a more fuller discussion.

11. For a more detailed discussion of "cultural sovereignty" consult the Cultural Report, Chapter 2.A and On-Line Report, Chapter D.14.

12. The term "electronic cultural heritage" is relatively new and was first coined in J. Knoppers, "Archives and Transborder Data Flows" paper presented at the International Association for Social Science Information Services and Technologies, Washington, 2-4 May 1980. The term is used to designate that part of the cultural heritage which exist in digitized or machine-readable form as distinct from the more common hard-copy or physical cultural products and recognizes the merger of artifact and information into one electronic digitized form.

13. In both the public and private sector, large quantities of data exist in electronic form only even if they originated in hard-copy form.

When the data is required it is recalled to the screen of the CRT or printed in hard-copy. In the public sector, unemployment, pension, welfare as similar social program data once verified are entered and maintained in a computer data base. A more recent example of information existing in electronic form only would be videotex data bases, (e.g., Telidon).

14. Relatively very few data files exist containing Canadian data that are readily available for use for instructional purposes, - where the data has been "cleaned-up" and adequate documentation with code- books prepared. The demise of the Data Clearing House for the Social Sciences in 1979 means that even if such Canadian data files do exist, knowledge of their availability is not widely disseminated.

    The result is that a professor teaching quantitative methods in political science very likely uses readily available U.S. data on voting patterns in a U.S. State to teach the methodology, thereby, foregoing the opportunity to combine the teaching quantitative methods with a study of certain aspects of Canada's development. See further, the Cultural Report and On-Line Report.

15. While a number of public institutions such as federal and some provincial governments, some universities and research institutions do have archival programs of which machine-readable or digitized data files form an integral part of such programs, most organizations do not. Organizations of all kinds often proudly display their first corporate ledgers or letter books, some well over fifty years old. Their first data files and data base or management information systems will be as interesting to the business historian of the future as are the manuscript ledger books to his counterpart today. See also below Chapter E.1 "Data Storage".

16. There was a case two years ago where a major international labour union (e.g., U.S.-Canada) decided to establish a labour history archive for the union in the U.S. This included shipping all non- active files from the various union locals to the central labour archive. Concerns were expressed in Canada about the removal of these files since:

    - workers who wished to sue the union (e.g., in relation to health cases dating back to the 1930's) would have to go through complicated legal proceedings; and,

    - those wishing to study the labour history of Hamilton, Oshawa or Sudbury would have to go to the U.S. to research this Canadian data.

    It was only through the professional dedication of a Canadian business archivist that the union was made aware of these concerns and a solution was found based on the microfilming of these manuscripts.

17. The On-Line Report provides a full discussion with statistical data and various appendices including the first "Compendium of Reference Data Bases currently accessed by Canadians".

18. See On-Line Report, Chapter B "Industry Structure and Trends".

19. The difficulties and validity of this concept are discussed in the Cultural Report, Chapter 3 and the On-Line Report, Chapter D.14.

20. See On-Line Report, Appendix 7.

21. Idem. See also, G. Deschatelets, "A Survey of On-Line Search Service Centres in Canada, Laval University, March 1980 (mimeographed report).

22. Based on S.B. Lawton, "The Diffusion of Automation in Post-Secondary Institutions", Canadian Library Journal, April 1981.

23. On-Line Report, Chapter D.14 and Appendix B.

24. Chapter II.D summarizes a much more extensive and fuller treatment of vulnerability issues as found in the Vulnerability Report.

25. Idem.

26. Ibid. See Chapter C and Appendix A and B.

27. Idem.

28. The recent introduction of "computer crime insurance" as a specialized type of insurance initially by Lloyds of London and now some U.S.-based insurance firms as well indicates a recognition of potential loss and an accompanying willingness to pay the insurance premiums.

29. This point permeates the Vulnerability Report.

30. Vulnerability Report. See the discussion of the Swedish, British and U.S. studies in this area. Sweden has such a program already well underway.

31. See Vulnerability Report, and especially Appendix C - "Encryption and other Scrambling Methods as a Means for Reducing Vulnerabilities in Various Types of Data Flows".

32. See Vulnerability Report, Chapter H.5.

33. See Vulnerability Report, Chapter E.1.b and footnotes 26 and 27.

34. For a more detailed discussion of the transborder data flow issues arising from the use of remote on-line diagnostic and repair services, see the Vulnerability Report, Part I, Section E.2, "Other Vulnerabilities-Personnel".

35. For further details, see the Vulnerability Report, Part I, Section E2, "Other Vulnerabilities-Personnel". It may be noted that during the time of debate on the Vredeling proposals during 1982 that their stridency and hardness have already been somewhat muted.

36. Neither time nor resources of the Task Force allowed for carrying out of this important task. Further, the U.S. report became available when the work of the Task Force was already well underway and the work program established.

37. For a more detailed discussion and analysis of data retention and data storage see the Data Report.

38. See Data Report, Appendix A which includes a set of preliminary observations and comments as to the preciseness or lack thereoff of the law or regulation on the question as to where the records in question must be kept.

39. For example amendments proposed in 1977 to the Combines Investigation Act apart from including machine readable data in the definition of "books, records, etc" would grant the Competition Policy Advocate the power to (under Section 10(1)(1)) "Examine, copy or take away ... any thing on which information on which information is or may be recorded". While Section 10(2)(1) speaks of "Everyone who stores data in a computer data bank, wherever situated, data related to business carried on by him in Canada and who acquires premises in Canada..." and later on, "where data is retrieval by means of terminal instrument located in Canada...". See further the Data Report.

40. The proposed Bankruptcy Act addresses the transborder data flow question head-on when it states in Section 53(b)(8) that "The Superintendent may ... require any one who stores in a computer data bank, wherever situated, data relating to a business carried on by him in Canada to supply the Surintendent ... which a print-out or other copy of any data so stored that it is retrieval by means of a terminal instrument, wherever located, in any form in which data can be retrieval and any print-out or other copy so supplied in intelligible write form ...". See further, the Data Report.

41. For a more detailed discussion consult the Legal Report.

DATE DUE

MAY MAI 26 1994			
SEP - 9 1998			

BF
BG
BD
BU
BP
SP
AC
TO