E

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

Directorate for Science,
Technology and Industry

Working Party on Information,
Computer and Communications
Policy

DSTI/ICCP/78.21

RESTRICTED

Paris, 28th July, 1978

Or. Engl.

Special Session on Policy Implications of Data
Network Developments in the OECD Area

from 13th-15th September, 1978

TRANSBORDER DATA FLOWS:
REQUIREMENTS FOR INTERNATIONAL CO-COPERATION

by

Ithiel de Sola Pool
and
Richard J. Solomon

Research Program for Communications Policy
Massachusetts Institute of Technology
United States

Acknowledgements

Among many whose advice has been helpful to us are Harry S. Bloom, barrister, Clark Hamilton, Library of Congress, Anne Branscomb, attorney, and our sponsors at OECD, Hans Gassmann and Dieter Kimbel. Richard J. Solomon is a Research Fellow in the Program for Information Resources Policy, Harvard University.

P R E F A C E

The emergence of national and international data networks raises new problems for governments, users and operators of these systems. The policy issues in transborder data flows have been treated at a Symposium on "Transborder Data Flows and the Protection of Privacy" organised by the OECD and the Austrian Government in Vienna in September 1977.

The international privacy protection issues are treated in the OECD by a new Expert Group on Transborder Data Barriers and the Protection of Privacy set up by the Working Party on Information, Computer and Communications Policy early in 1978.

In order to further explore and clarify international policy issues in transborder data flows other than privacy protection, a Special Session of the Working Party on ICCP will be held on 13th-15th September, 1978 at OECD Headquarters in Paris.

The Organisation has asked Professor Ithiel de Sola Pool of the Center for International Studies, Massachusetts Institute of Technology, United States, to prepare a report which should serve as a background document for this meeting.

We wish to thank Messrs. I. de Sola Pool and R.I. Solomon for the preparation of this report. The opinions expressed in it are those of the authors alone and do not necessarily represent the views of the Organisation.

Table of Contents

SUMMARY OF CONCLUSIONS

Legal and political impediments threaten to obstruct the development of useful transnational data services. The purpose of this paper is to explore how the community of industrialized nations can avoid these impediments. We ask how far problems can be ameliorated by reaching international agreements or common standard, and also seek to identify those issues in which common rules, though they may appeal to some intellectual sense of orderliness, fail to meet the test of compelling need and mutual advantage. One issue, that of privacy, has already been much studied and is hence excluded from our treatment. The question here is whether there are other issues besides privacy that may require systematic investigation, the question is asked, whether international understandings are needed to protect the security of non-personal data. Such a formulation is too restrictive. For commerce in information to thrive, new legal and commercial practices will have to evolve, but not just for confidentiality. Creators and vendors of intellectual property must be paid and must be able to enforce the contracts they make. Trade in a commodity as fluid as computer data transmitted by telecommunications requires different commercial institutions and practices than does trade in physical goods, or even books and films. In time the industry will discover and work out payment schemes, liability arrangements, and ownership definitions appropriate to its unique technology.

International organizations such as OECD can assist that process of exchange of experience to work. International agreements may play a role in establishing comity in law enforcement, and also for facility planning and setting of technical standards. However, what will not work in the new technology of data communication -- without total censorship -- is an attempt to control the content of the bit stream of data that traverses national borders.

Criteria:

In evaluating the importance of reaching international agreements on data flows, we apply six main criteria: (1)

1. Public good.

2. Minimize international action: Even if it be concluded that social welfare will be served by action, we postulate that in a world of nations, unless there is some compelling need for coordination, action should be left to each individual nation.

3. International agreements should generally sustain rather than supplant domestic laws.

4. Avoid unenforceable laws.

5. Regulate negative externalities: The main justification in free countries for government regulation is that innocent third parties are likely to be hurt.

6. Regulate the abuse, not a single means that sometimes is abused.

A number of proposals have been made for international regulation of transborder data flows. Some of these proposals stand up

---

(1) See Foreword

against the criteria that we have listed and some do not. We list first some proposals that present problems:

1. Treating legal persons as identical to real persons: Most privacy laws and other proposed regulations on transborder data flows are limited in their application to data about real persons. The suggestion has been made that they should apply also to legal persons for at least some purposes. Whether any particular regulation should be applied to legal persons is a question that should be answered in its own right on the basis of the particular facts. It is generally recognized that it is no solution to mechanically apply a legal fiction. (Sec. 1.3.3)

2. Rigidly distinguishing computing from communication: That too is a distinction in which legal words of art do not correspond to the empirical reality. (Sec. 7)

3. Regulating the content of what may be carried on particular circuits: With the emergence of all-digital systems and cheap effective encryption devices, there is no technically practical way to distinguish whether any particular message is voice or data, messages or computation, in-house or to third parties. (Sec. 2.1, 2.2, 6.3, 6.4 and 6.5)

4. Protecting the security of non-personal records by international standards: Security costs money. There is a trade-off available to any organization to have more security for its computerized records for more cost. The main reason for a government to compel an organization to acquire more security for its records is if that organization is acting as a fiduciary for third parties. Governments will differ in the extent to which they wish to protect third parties by mandatory security standards or by legal liability. (Sec. 4, 5, 6.2)

5. Conventional copyright: While it is important to develop new ways of compensating the creators of intellectual property in the computer age, it is clear that the traditional notion of copyright inherited from the printing press will not work with computer records. The mechanism of enforcement that underlay the traditional notion was the fact that large numbers of uniform copies were produced at a single place, the printing press. Computer records are dispersed, infinitely varied in content, displayed in forms ranging from printout to CRT display, and often used without any display at all. (Sec.8)

Proposals that are worth consideration: (1)

Among the proposals for international agreements concerning transborder data flows that are worthy of consideration, there are a few in which it would seem necessary or desirable to reach international agreement on actual details of what is done and what is not. We note four such areas:

1. Technical standards: CCITT is already operating in this area; there can be little doubt that its work is important. (Sec.2)

2. Encryption: One standards agreement that would be particularly important for protection of privacy and security would be one guaranteeing the right of users to encrypt their material. If there are to be networks with random routing, such as packet nets, then all nodes must allow passage of encrypted data. (Sec. 2.2 and 6.4)

3. Origin identification labels: (Sec. 5)

4. International capacity planning. (Sec. 3)

Aside from these rather limited (albeit important) topics the kind of co-operation that seems to be required (and that needs to be put on the agenda for discussion among nations) is agreement to support the domestic law of different countries against attempts to evade them by operations from a distance carried on across a border. One can imagine useful agreements of this kind

(1) There is one set of regulations the legitimacy of which is widely recognized, but which we do not consider in this paper, namely controls applied for reasons of national security. Those are generally applied by single countries or alliances rather than by international agreement, and they sometimes require significant departure from what would otherwise be viewed as desirable public policy. That raises an entirely separate set of issues.

being reached regarding several related matters. The essential condition for this kind of agreement is that all parties to it regard a particular genus of action as illegal, but that the details are left to each to carry out in its own way. (Sec. 6.1)

Among topics on which such agreements might be considered are:

1. Locus of liability: If in an illegal activity or contractual liability, data is physically located in one country but accessed from another, where has the offense taken place and who prosecutes or sues? (Sec. 6.2)

2. Computer fraud: While much less of a problem than some popular journalistic treatments suggest, computer fraud is a problem. To help meet it, countries could agree to each incorporate into its own domestic law a provision making it illegal to knowingly access a computer in another country for the purpose of carrying on certain specific activities that are illegal in that remote country. Among kinds of activities that might be listed are such ones as seeking personal information from a data base to which the receiver is not entitled by the laws of the host country, withdrawing funds from an account to which he is not entitled under the laws of the host country. (Sec. 5 and 6.2)

3. Illegal use of computer facilities at a distance: The purpose of this provision is to enable facility owners to enforce their usage charges and to prevent illicit access to private facilities. (Sec. 6.2)

4. Contract enforcement: To facilitate the enforcement of contractual agreements between computer or file owners, on the one hand, and their users abroad, countries could adopt laws to give recognition to liabilities incurred under such agreements. (Sec. 6.2)

5. Relationships of public trust: There are certain institutions that have a special relationship of public responsibility to their customers. For example, banks, doctors, airlines. In some such situations of public trust there could be evasions based upon transborder telecommunications operations. Since these standards are specific to particular areas of activity there is no way of reaching general conventions or standards; agreements have to be field by field. The two fields in which causes for concern have begun to arise, and which might be fruitfully discussed in the near future are privacy and EFTS. (Sec. 6.2)

6. New concepts of copyright: Ways must be found to compensate creative intellectual activity. It is in the self-interest of both creator of software and of users that there be payments for creation. The system of payment that will ultimately develop out of this mutual self-interest cannot yet be anticipated. It is not premature to study the problem. It seems likely to take a decade or more of study before the shape of appropriate solutions will become clear. (Secs. 8 and 9)

7. Payments system: The costs of furnishing on-line information services fall into three categories: (1) creating the information and converting it into machine readable form; (2) maintaining it in a computer; (3) searching it and transmitting the information requested by a customer. The bulk of the costs lie in the first category, while collection from the ultimate customer takes place in the last.

The problem is to devise payment systems that collect reliably, distribute the ultimate payment back to the various contributors, and enable small customers to establish their credit easily and at the moment that they wish to access the data base. Collection by the telecommunications carrier is one way that meets many but not all of the problems. The design and development of an international payment system for data base access is an important subject for study by international organizations. An effective payments system would be a major contribution to the growth of international computer co-operation. (Sec. 10)

It should be emphasized that identifying a topic as appropriate for discussion is not the same thing as advocating the adoption of any particular agreement. The purpose of this paper is to define an agenda. It is not to advocate particular answers.

FOREWORD

In this paper we note

--some problems affecting transborder data flows,

--some options available for coping with these problems.

The options that we analyze most closely here are those that for implementation require international co-operation.

Administrations must cooperate in a variety of ways if a data communication system is to operate effectively between nations. In this paper we deal with some of the necessary kinds of cooperation but let us first schematically note the range of types of cooperation required, and indicate those with which we propose to deal.

First, both nations must permit such communications. A commitment to such freedom exists among OECD countries. They recognize that it is inappropriate for governments to restrain their citizens from communicating as they wish and furthermore that international communication contributes to productivity. Some other states do censor private transborder communication: but in OECD countries that is an activity that national administrations facilitate.

Second, to transmit data across borders requires co-operation on standards. We discuss this matter only briefly for it falls primarily in the domain of other organizations than OECD.

Third, for transborder data flows to be economically viable there must be a method for collecting and sharing payments for facility use. We shall discuss this matter to some extent.

Fourth, transborder data flows become entwined in legal issues concerning privacy, intellectual property, national security, and economic policies. Some of those issues are the central focus of this paper.

We shall not deal fully with the issue of privacy, for that important issue has been the subject of previous OECD treatments. We touch on it, however, in Section 1.3, and elsewhere, because it provides a reference point with which we can compare various other political and legal issues which are our principal topics.

Criteria of judgment:

Laws and policies of countries differ. One premise of a system of nations is that in the absence of compelling considerations to the contrary, countries go their own way. Our presumption is against unnecessary standards or demands for uniformity. However, there clearly are substantial areas in which interdependency and international externalities exist. In such situations all parties may gain if they can agree on practices.

Criteria:

In evaluating the importance of reaching international agreements on data flows, we apply six main criteria:

1. Public good: In the absence of any compelling judgment as to what is desirable or undesirable, free governments will leave to the citizens to do as they choose. Yet in an exercise of this kind avoid value judgments. Every proposal for regulation implies a judgment that social welfare will be served in an important way.

2. Minimize international action: Even if it be concluded that social welfare will be served by action on a problem, we postulate that in a world of nations, action on a problem should be left to each individual nation, unless there is some compelling need for co-ordination.

3. Most international agreements should sustain rather than supplant domestic laws: Some international agreements, such as those setting engineering standards, constitute a kind of international legislation (even if they have to be nationally ratified) in that they reach a fixed conclusion as to the content of what should be done. Other international agreements, such as copyright conventions, usually just provide a mechanism by which laws adopted in different countries can be made effective against evasion abroad. Under the principal of minimizing international action, preference should be given to agreements that sustain domestic laws, if that will do the job.

4. Avoid unenforcable laws: Where action is needed, it should be done in ways that the technology makes practicable. Legal declarations that come to be widely disregarded cause a decay of moral habits and of the credibility of the system. As technologies change, one must change the means of enforcement to ones that are pratical for the enforcer, not invitations to violation.

5. Regulate negative externalities: The main justification in free countries for government regulation is that innocent third parties are likely to be hurt by agreements between others. For mature adults, it can be assumed that agreements they reach are in their own best interests and need not be controlled. Privacy laws are classic examples of regulations to protect people against agreements that others reach, but which affect unwitting and unwilling parties. But rules on how a business secures its own records <u>for its own protection</u> on the other hand would cannot be justified by this criterion.

6. Regulate the abuse, not a single means: To control an abuse by regulating one particular means by which it is sometimes perpetrated results both in barring many innocent actions that may use the same means, and in allowing the perpetuation of the same abuse by other means. Thus regulations designed to protect privacy, but which merely bar certain computer systems, may both deny others the legitimate use of those systems and also permit the same abuses of privacy through alternative means such as the mails. Desirable regulations are quite specific as to the content of what one wishes to control, not just regulating the mechanism.

A number of proposals have been made for international regulation of transborder data flows. Some of these proposals stand up against the criteria that we have listed and some do not. The purpose of this paper is to examine such proposals. We try to identify those legal and political issues concerning transborder non-personal data flows where there would be mutual gain from reaching agreements, and at the same time to identify issues in which common standards, though they may appeal to some intellectual sense of orderliness, fail to meet the test of compelling need and mutual advantage. Many laymen's concerns about computers have little to do with reality. Some concerns reflect the psychological trauma of coping with any massive change, and also the age old human anxiety about machines that seem to take on features of intelligent life. At first computer Frankensteins were expected to create unemployment, but early studies usually found that they created more jobs than they eliminated. Today, a quarter of a century later, those early expectations have more support, but even now the picture is not clear. (1) Science fiction writers dreamed up machines that

(1) Prof. C. Freeman is currently engaged in a study for OECD for which as yet the data is not in; there is still only a statement of his hypothesis. He notes in his planning document that a couple of decades ago, unemployment consequences of the

would triumph over human intelligence, but then real computing machines were found to be essentially dumb. Now there is a general anxiety about computer invasions of privacy; but there is reason to expect privacy to be better protected in computer files than in manual ones. Yet computers and computer communications do involve new problems. Our task is, in part, to separate out the hallucinations from the real problems.

When real problems hav been identified, the proposed solutions need to be looked at with the cold eye of cost/benefit analysis. The word "problem", after all, implies much more than that something is an unmitigated evil. A problem is a dilemma; it is an undesirable aspect of something that is wanted. Pollution is a byproduct of the goods of civilization; unemployment may be a byproduct of improved productivity; invasions of privacy are a byproduct of increased knowledge. The "solutions" to problems can easily destroy what is wanted along with eliminating the byproduct. Solutions, like medicines, have side effects, and so

---

electronic revolution seemed so obvious that the American, British, and Soviet governments all appointed special commissions on the problem. Careful research, however, showed the Cassandras to be wrong at the time. Professor Freeman lists several possible reasons for the error, and offers the hypothesis (to be tested in his research) that the correct reasons were some transitory ones related to the stage of a product cycle in which the electronic revolution was at that time. His speculations note that electronics at that time introduced several major military and consumer products (e.g. radar and TV), but that today electronics is beginning to penetrate other branches of industry in labor saving applications.

If the data comes out to support this hypothesis, then the employment implications would be adverse, while productivity would, of course, increase.

they too are dilemmas. They may reduce negative consequences, but in turn have costs. So in looking at problems associated with transborder data flows, it is not enough to simply list dangers and options for their solution. We must also note the problems (i.e. costs and undesired consequences) of the proposed solutions too.

It should be emphasized that identifying a topic as appropriate for discussion is not the same thing as advocating the adoption of any particular agreement. The purpose of this paper is to define an agenda (1) It is not to advocate particular answers. We define the agenda by applying a set of criteria to a set of proposals to see if they are worthy of study at all. We have identified some proposals that do deal with serious problems and would do so in ways that conform to the normal processes of international co-operation. Having met that criterion of acceptability, a topic belongs on some agenda, but much deliberation remains to be done before either we as authors of this paper, or the nations that must deliberate and decide, reach a conclusion as to what in particular should be incorporated into any international agreement.

---

(1) There is one set of regulations the legitimacy of which is widely recognized, but which we do not consider in this paper, namely controls applied for reasons of national security. Those are generaly applied by single countries or alliances rather than by broader international agreement, and they sometimes require significant departure from what would otherwise be viewed as desirable public policy. That raises an entirely separate set of issues

A matter that we do not address in this paper is the appropriate forum for working out an international payments system, or developing a new mechanism for protecting intellectual property embodied in computers, or for discussing agreements to extend comity to the data-related laws of foreign nations. A number of international organizations are certainly involved. Among them OECD is important as the organization of the countries most heavily engaged in international data flows. It can and should take initiative in a number of the areas where action is worth considering.

1. INTRODUCTION

1.1 The Importance of International Data Communication

History, in evaluating our era, may well view as one of its signal achievements the erosion of economic and technical barriers to the instantaneous exchange of information among persons who are far removed from each other, and regardless of frontiers. Since communication costs by satellite have become almost insensitive to distance, and transmission time no longer a barrier to interaction, unprecedented opportunities for international co-operation arise.

In societies in which information activities generate up to half of the GNP, substantial gains in productivity will arise from efficiency gains in that sector. (1) Thus there is good economic reason to use the cheapest, fastest, most accurate, and most complete information facilities available, wherever they may be located. Just as international trade in physical commodities has raised living standards in the world community by allowing use of commodities produced in the most advantageous place, so societies half of whose economic activities consist of information operations will gain mutual advantage from shared use of information resources, with each nation working especially at activities in which it has a comparative advantage. Energy and

(1) Cf. Simon Nora and Alain Minc, Rapport sur l'informatisation de la société, Paris: Inspection Generale des Finances, 1978, Part I Ch. 1.

other scarce resources can be saved by linking distributed activities electronically, rather than duplicating expensive facilities in many physical locations; examples of such energy-saving uses of communication include teleconferencing, specialization among libraries, and integrated inventory management.

Most important of all, creativity flourishes when human beings can interact across physical barriers in the pursuit of science, culture, and personal affection. The nations of the world have recognized this fact in a series of agreements to encourage cultural exchange and the free flow of information. Among them may be noted the UNESCO Charter, the Universal Declaration of Human Rights, and the 1950 Florence Agreement on Importation of Educational, Scientific, and Cultural Materials. The latter exempts such materials from customs duties when imported for non-commercial purposes and commits the signatory states to "promote by every means the free circulation of educational, scientific or cultural materials and abolish any restrictions to that free circulation." (Article IV) A Protocol to that Agreement adopted in Nairobi at the UNESCO Conference of 1976 explicitly adds to the list of materials covered by the agreement "magnetic or other information storage media required in computerized information and documentation services." The signatory nations have thus already agreed to seek to abolish restrictions on the import of data for scientific and educational computerized data bases.

Figures 1 and 2 show the extraordinary current growth in the volume of usage in data base retrieval services. Figures 3 and 4 are drawn from one among the several forecasts that have been made of the continuing growth in data communication, this one from Japan. (1) There is a similar explosive growth in most forms of international telecommunications. The FCC has estimated the annual growth rate in international leased line data circuits at 21%. (2)

Throughout the industrialized world packet nets and other data networks are opening up for service. The airline net was the pioneer. SWIFT, the bank clearance network, has just gotten under way. Euronet goes into service in the coming year. In Japan KDD is moving rapidly toward the implementation of its Venus packet net, to be linked in about a year later to a domestic net. There, as in all the major European countries, arrangements have been made within the last year for international data transmission services, that permit users in all industrialized countries to access the world's major data bases through switches at their own PTT's and via the various competing American international record carriers and the specialized value added carriers there. The costs of communication have already fallen to the point where numerous users choose a computer or service bureau.

---

(1) Research Institute of Telecommunications and Economics, Prospects of the Demand for Data Communication, 1977.

(2) Dataphone Inquiry, FCC Docket No. 19558, p. 3.

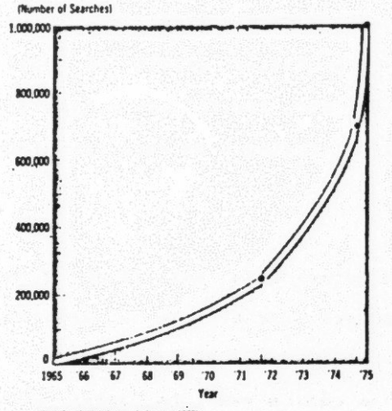


FIGURE 1

* "Statistical Indicators of Scientific and Technical Communication: 1960 1980" by D. W. King. Report for the Division of Science Information, National Science Foundation, 1976.

FIGURE 2

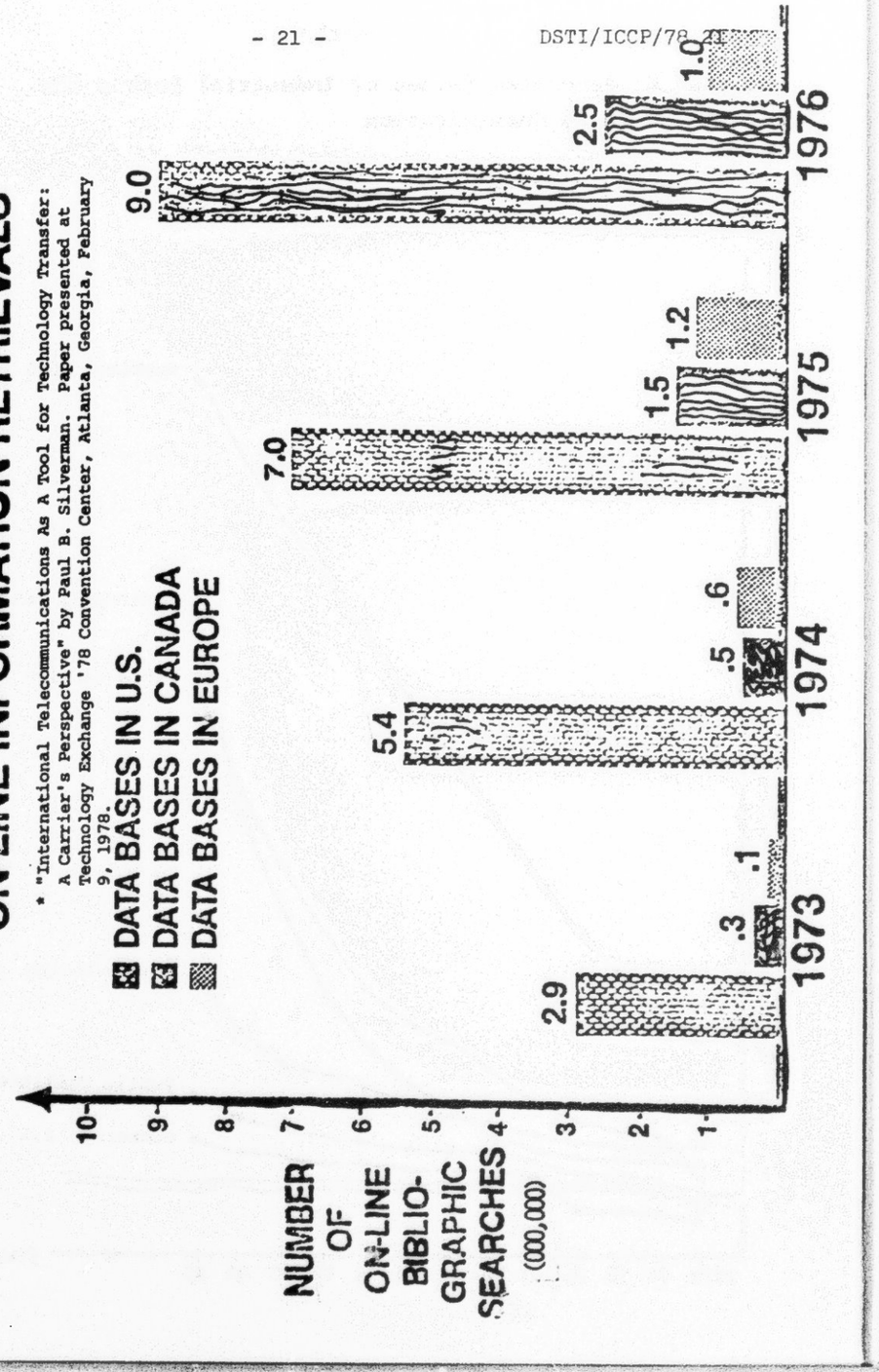


Figure 3 Predicted Values of Industrial Demand for Data Communication

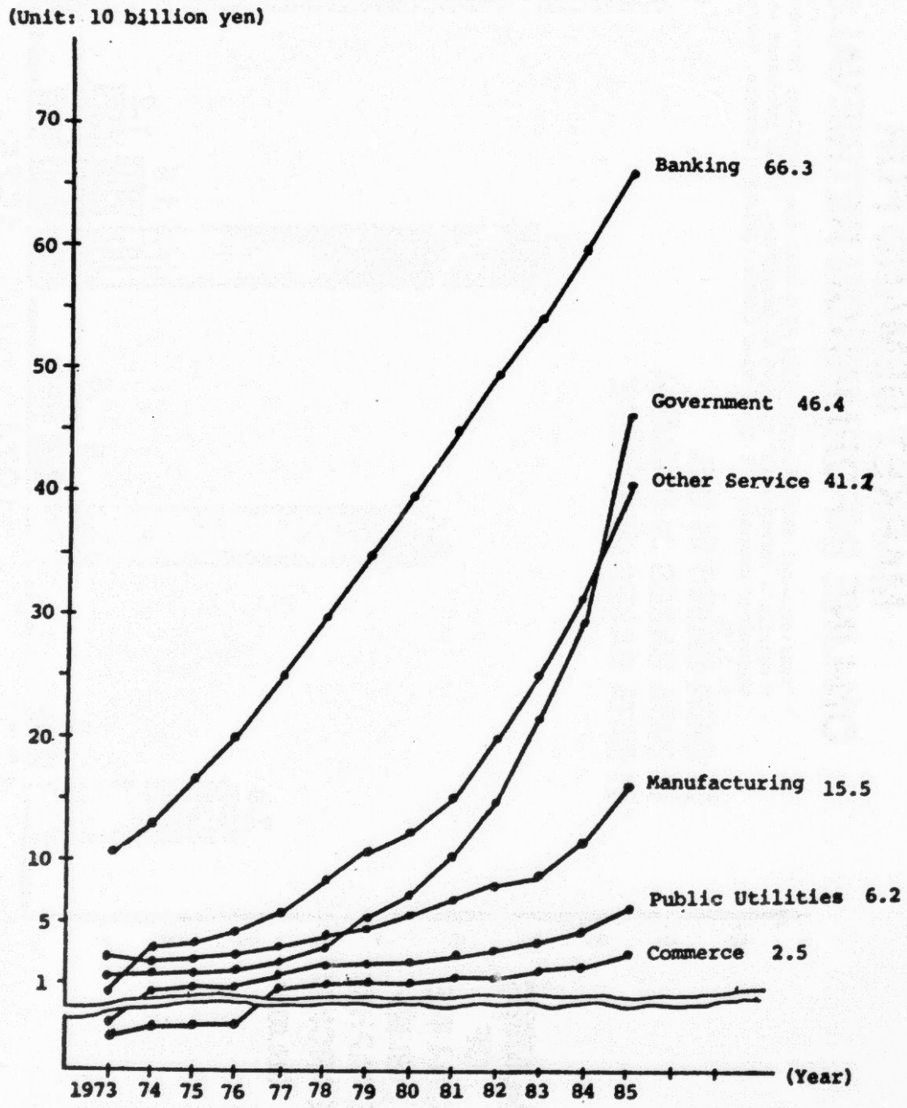
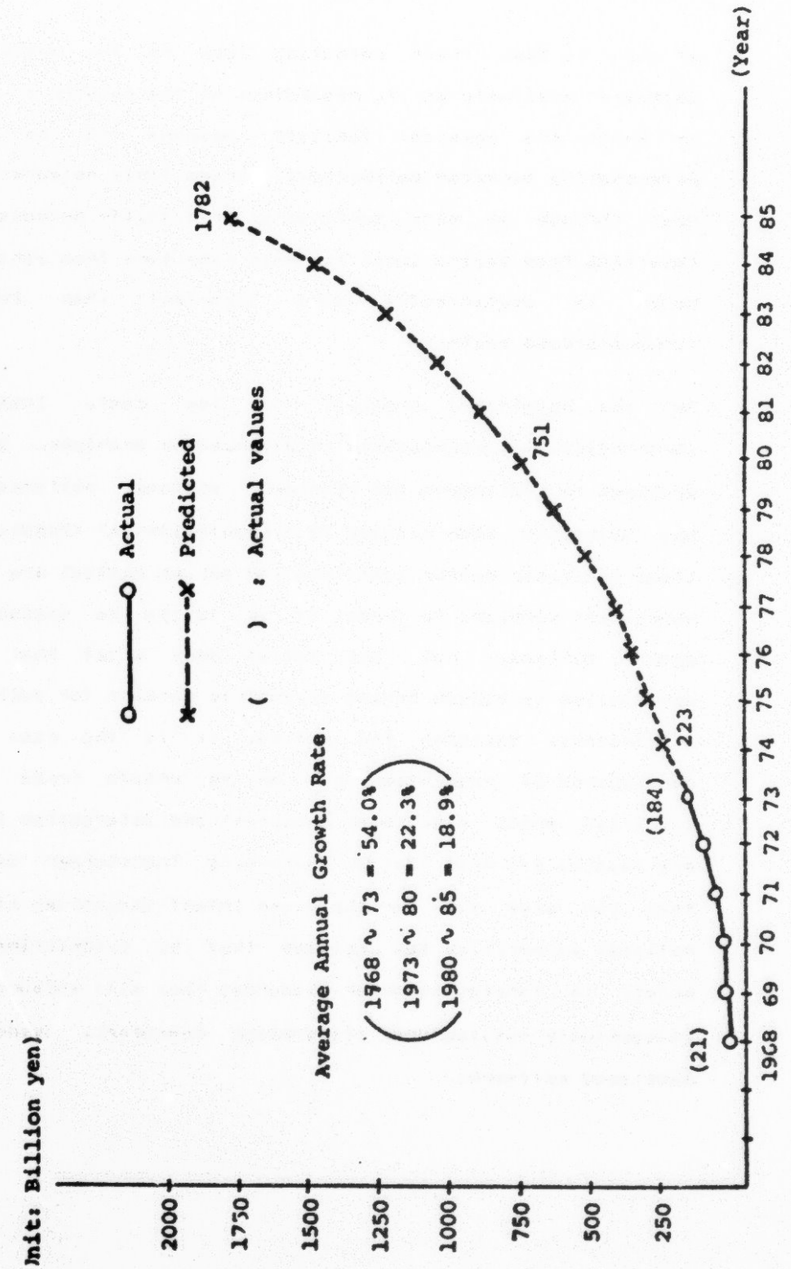


Figure 4 Total Demand for Data Communication



at which to have their computing done on the basis of the software available on it, regardless of the country or continent in which the physical facility happens to be located. Time-sharing services deliberately spread their networks East and West through as many continents as possible because the load levelling from having input to their computers from various time zones is economically more important than the extra communications costs.

Yet the beneficent prospect of low cost, instantaneous international communication is attended by problems. One of the problems is continuing and resurgent economic nationalism. It has sometimes been alleged that regulations of transborder data flows (whatever better justification may be stated) are used as a non-tariff barriers to trade. It is futile to speculate thus about motives, but the belief does exist that economic nationalism is hidden behind ostensible concern for such matters as privacy. Whatever the motive, it is the case that one consequence of regulation can be to create trade barriers. Countries whose electronic equipment and information industries are lagging may hope that by burdening transborder data flows they can give time for their own infant industries to develop. National authorities may believe that by restricting network access to foreign computer resources they will encourage use of indigenously manufactured stand-alone computers, using locally developed software.

Of course, the effect of protectionist measures may be just the reverse. If the domestic information industry and the local applications programmers are denied the opportunity to use the best computers, software, and data bases that exist, that restriction may well inhibit the growth of computer skills and computer usage in a country. It has often been the case that restriction on the computers and software that are available for use, results in customers choosing to continue to doing things in old-fashioned manual ways rather than pressing forward to innovation. It may result in technicians in that country failing to master the full state of the art. Using clumsy and limited systems is rarely the path to growth.

1.2 OECD's Role

Intelligent policy making about such complicated matters is not easy. What seems obvious is not always right, and the consequences of unsound policies can be great. Careful study in respected forums such as OECD in which the major actors are all present, is called for, lest ill-considered policies be adopted. Certainly, problems about data flows do exist, and will lead different OECD nations to legislate about some aspects of data communication. With policies being made by diverse jurisdictions, there will inevitably be problems to be resolved in carrying on transborder data traffic. How to reconcile the tensions between diversity of policies on the one hand and the

opportunities that international communication offer on the other, is the problem before us.

It is appropriate that OECD should address itself to that problem. While data communication is rapidly becoming a global phenomenon, it is still largely concentrated in the advanced industrialized countries. Furthermore, the fact that OECD nations share certain common policies and values will make it far easier to take the exploratory steps in resolving problems of transborder data flows than to do it on a global scale. The OECD nations share the view that ordinarily anyone ought to be allowed to communicate in a free flow of information, with anyone else anywhere; prohibitions are narrowly-defined legislated exceptions. The OECD members share too the belief that the search for knowledge by citizens is a desirable and free activity, limited only by specific rules to protect the privacy and property of others. They share also the system of private enterprise and are committed to open channels of commerce among themselves. They seek to expand, not contract, joint economic activity, and to realize joint gains in productivity.

In 1977, an OECD Data Bank Panel formulated those concepts clearly in a set of principles. (1) The first three of the five principles recognize the value of free transborder data flows:

(1) Summarized in the Secretariat's Note (DSTI/ICCP/77.46).

(i) Conditions for the continuous, uninterrupted flow of information among countries should be maintained.

(ii) Countries should ensure the maximum opportunity for the movement of information across borders, imposing restrictions only for specific and valid reasons.

(iii) Rules of fair competition should be applied to information resources and services, avoiding restraints in the form of non-tariff and other barriers.

The last two principles identify the area in which some regulation may be appropriate.

(iv) Appropriate data security and confidentiality requirements should be set up.

(v) Personal information should be protected wherever it resides, as it would be in its originating country.

We have been asked to explore in this paper the matter of data security and confidentiality and also whether there are other problems besides the two listed by the panel for which international regulation may be required. In general we think not. We concur with the judgment of the panel. We propose, however, a somewhat modified and expanded notion of what has usually been talked about as "security and confidentiality." What is at stake is the ability of data owners to enforce contractual arrangements that they make with others across frontiers. Unless

a legitimate owner of data can exercise some control over access to it, he will have no incentive to invest in data development. Every country in its laws about intellectual property, patents, and contract enforcement recognizes that fact. The problem cannot be resolved in the narrow technical context of physical security of computer data. It must be viewed in the broader context of industrial organization and law enforcement as well as technology. So in what follows we consider, not just such matters as technical standards for security or encryption, but even more such matters as the methods for international contract enforcement. The heart of the problem lies in international legal arrangements regarding locus of liability, computer fraud, payment arrangements for computer services, copyright, and fiduciary responsibilities.

We have identified, and listed in the Conclusions, some ten areas in which international co-operation is worth further consideration, all of which fall under data security as we have redefined it. Among those areas, one is that of technical standards, including permission of encryption. But the bulk of our paper is devoted to such matters as the extension of domestic law to check frauds perpetrated via telecommunication across borders, and to matters of intellectual property. Also as transborder data networks grow, co-operative means must be found to simplify payment for service.

To provide the reader with a guide to the topics with which we shall deal, note that we organize the treatment under the following headings:

Area of Regulation	
Engineering compatibility	Section 2
Capacity Planning	Section 3
Data regulation: for privacy	Section 1.3
for preventing fraud	Sections 4,5
Contract enforcement	Section 6
Intellectual property	Section 8
Payment systems	Sections 9, 10

For each of the above areas we shall try to identify the type of international action that is appropriate to problems in that area. We classify the types of action as:

Individual action, i.e. no formal international action beyond discussion

Comity in law enforcement

Setting of standards

International organization.

Without offering further explanation or justification at this point we tentatively list the major conclusions as to how these approaches most nearly fit these topics, leaving out two cells for which the answer requires fuller explanation..

Area of regulation	Type of international action	
	For data on Real Persons	For data on Legal Persons
Engineering compability	- Standards -	
Capacity Planning	- Organization -	
Data regulation: for privacy	?	Individual action
: for preventing fraud	?	Comity
Contract enforcement	- Comity -	
Intellectual property	- Comity -	
Payments Systems	- Organization -	

1.3 A Comparison of the Issues Concerning Privacy and Security of Data About Real and Legal Persons

1.3.1 The case for harmonization of data regulations

Until now, OECD deliberations on transborder data flows have focused, quite properly, on the movements of personal data. (That is the problem of "privacy.") There are good reasons for OECD's concern in this area, but that topic having been extensively explored, it is not the assigned subject for this paper. Our subject is policy issues about non-personal data (often discussed as "data security," or "proprietary.") We devote a few pages here to comparing the two issues, their similarities, differences.

Most industrialized countries have already passed, or are now considering laws to curtail abuses of automated files containing personal information. (1) There is widespread concern about the

(1) The Secretariat note mentions steps in Sweden, the USA, Germany, Canada, France, Austria, Belgium, Denmark, Luxembourg, the Netherlands, Norway, Spain, Australia, Ireland, Italy, Japan, Switzerland, the UK, and EEC. The German and American laws concern manual as well as automated files. The other laws, in general, deal only with computerized files. One may question the rationale for regulations to assure privacy that are applied to files in computers, but not to other files. If an abuse needs to be controlled, it presumably needs to be controlled regardless of the technology used to perpetrate it. Most of the laws, however, cover any sort of personal file in a computer, sometimes with specified exceptions such as address lists. An approach that focused on the feared abuse would presumably apply different regulations to a credit bureau, a hospital, the income tax bureau, and a reporters private notes. Since our paper's topic is not privacy, we do not go into this matter in more detail, but the reader may note that we have followed this approach in discussing non-personal data. A good deal of our discussion is about banks. It would seem that data files that in effect change assets and liabilities of others need quite different treatment from non-personal files that only contain information.

power that can be exercised over ordinary persons by those with access to computerized records. (The new Norwegian and Danish privacy laws apply to legal as well as real persons and then only in some respects.)

The problem which such laws address can be stated in terms of the economic concept of a negative externality, which is the classic situation in which government action is justified. In calculations of welfare, account must be taken not only of the value received by employers and employees, or buyers and sellers, from the deals that they conclude with each other, but also to the adventitious costs and benefits that accrue to third parties. When information is sold by one party to another, the buyer and seller each get their benefits from the deal they make with each other; but if the information describes a third person or organization, they stand to lose or gain, too. Those incidental effects are externalities -- positive if others benefit, negative if they are hurt.

Transactions involving externalities need to be policed by some process beyond the discipline of the market. The buyer and the seller presumably look out themselves, and if they make a deal each expects to benefit. But they can hardly be expected to look

out for the interests of third parties. The law, normally, has to do that, restricting thereby the freedom of the buyer and seller on the bargains which they may make.

Regulations on personal data ordinarily concern a situation in which the third party may be relatively powerless compared to the organizations that buy or sell the data. A credit bureau, for example, sells data about a customer to a merchant, or a police administrator releases data on a person to an investigator. Traffic in information about organizations or governments seldom involves such an imbalance of power. Indeed at precisely the same time as governments are adopting privacy laws, in many countries they are also adopting sunshine laws to force governments to conduct more of their transactions in public. The contradiction has been most apparent in the USA where the Privacy Act and the Freedom of Information Act came at almost the same time and forced major, but opposite, revisions of administrative procedures. (1) Public officials are now obliged to show anyone who asks all but a few exceptional documents from public files, but at the same time (as one of the exceptions) private information about individuals is more strictly than ever enjoined from being shown to others, even other agencies of government. Clearly a different value judgment is being applied to information about individuals and information about government agencies.

(1) Canada is also now debating a sunshine law.

1.3 Conflicting considerations:

International agreements establishing uniform standards about either privacy or propriety will not be easy to achieve, even among democratic countries, because there is no unanimity among them on the balance among conflicting considerations. We shall discuss below some of the differences in national copyright practice. The same thing can be seen from the experience about privacy standards to date. There is indeed unanimity that privacy is a good thing, but so are other values that are in direct opposition to it, most particularly freedom of speech and enquiry, and the right of the people to know. Different countries will, undoubtedly, reach different conclusions about such sensitive matters as a newspaperman's right to keep his sources of derogatory personal information secret, or a citizen's right to keep his tax payments secret.

Some privacy laws have been adopted with little thought about these conflicting considerations. More recently, however, with more experience, there has been evidence of drawing back from more extreme privacy protection, particularly in Britain and the USA. In Britain, the Royal Commission on Privacy examined proposals for a "legal right of privacy" and decided against it, because it would oblige the courts to balance individual claims to privacy against the public's right to know. (1) In the USA,

(1) The Whitford report; cf. also Royal Commission on the Press, Chm. O.R. McGregor, July 1977, Cmnd. 6810, 9.9-9.12; "Computers: Safeguards for Privacy", Home Office, Dec. 1975, Cmnd. 3654.

the balance has been heavily weighted in favor of sunshine laws, such as the Freedom of Information Act. That protection of one man's privacy is the invasion of another's, became apparent when the US Congress adopted an act (the Buckley Amendment) giving students access to their university records. The protests of those whose letters of evaluation were thus compromised became so strong that the law has been largely negated. Students now are more or less compelled by their universities to sign waivers.

The strongest opposition to the new movement to give people access to files containing information about themselves has come from the press. Journalists suddenly became aware of the opposition between their right to compile data on people on whom they were reporting, and the claim of aggrieved people of a right to inspect and correct files upon them. In the USA, a Reporters' Committee On Freedom of Information has been formed, largely to combat attempts to compel them to reveal their sources and files.

One may conjecture that despite contradictions and oscillations, the United States will end up adhering to a tradition of "robust and wide open" debate, (1) with minimal libel laws and denying the right of individuals to control or correct what others choose to keep or transmit in personal files about themselves, except for some government files which will be extensively opened, and files in a few sensitive situations such as credit bureaus and personnel records. Some other countries will choose to seize the

(1) New York Times Co. v. Sullivan, 376 US 254, 1964.

opposite horn of the dilemma and will protect individuals comprehensively against the freedom of anyone to keep files with inaccurate or abusive personal information.

Some countries, particularly the USA, will stress protections of the individual against the power of government. (The American privacy law of 1974 concerns government files.) Other countries may bestow additional authority on government for the purpose of protecting individuals against corporations and other individuals.

Given these differences in perspective, any international agreement on personal information is likely to be at the lowest common denominator. It may give some important protection to privacy, but not as much as privacy activists would like.

Yet international agreements on some minimal privacy standards might well be justified. The problem is one that cannot be fully handled without international co-operation. The problem certainly constitutes a legitimate area of governmental concern, because weak individuals are inadvertantly injured by actions of other parties. And within limits, all democratic governments agree that something needs to be done that they cannot do alone.

On transborder flows of personal data, there is, at least, a basis for consensus. That fact has already become apparent in earlier OECD discussions. The degree of likely consensus on protection of proprietary information or other information about

large and powerful organizations is likely to be less than that about privacy.

1.3.3 The matter of "legal persons":

A highly controversial issue at the present time is the question of whether or not legal persons should be covered by data protection legislation. In the USA Congressman Goldwater has made some proposals to that effect. The issue was hotly debated in the French National Assembly before their privacy law was passed last year, without such extension.

It has occasionally been suggested, that simply as a matter of the logic of the law, if regulations protect persons, then by the same argument, legal as well as real persons should be protected No countries, however, have as yet taken such a formalistic position. Legal persons are not real persons; if they are treated as such in some laws, it is because for some purposes it is convenient. Such inclusion requires more justification than verbal legerdemain. Corporations and institutions are different from real persons in many respects including wealth, power, and need for protection. The Norwegian and Danish laws which cover data about both real and legal persons make relevant distinctions. (1) The arguments, if there are any, for protecting the confidential information of organizations along with the confidential information of real persons, have to be

(1) In the Danish case there are two separate laws.

made in their own right, and not by automatic application of a legal fiction. The question as to what kinds of public actions are appropriate for the protection and regulation of data about legal persons is a subject that OECD and its member nations will be discussing, and indeed are what the present paper as a whole is about.

2. ENGINEERING STANDARDS: A PREREQUISITE TO INTERNATIONAL COMMUNICATION THAT CAN SOMETIMES ALSO BE A BARRIER

One area in which international conventions are clearly necessary, if international data communication is to flourish, is that of engineering standards. CCIR and CCITT have been the main fora in which such standards are set. Data transmission has long occurred over the existing public switched network of telex and telephone and over leased lines. For the public telephone network, inexpensive, low-speed modems can be readily attached with no additional system modifications needed. With leased lines, data transmission can be even simpler since lines can be ordered with specific characteristics adjusted for low-speed data with or without modems. Changes are now occurring in the increasing need for optimized high-speed, error-free data networks. To keep pace with computer technology, new agreements on standards (such as the high-level data protocols, X.21 and X.25) and new facilities will be required.

2.1 Voice vs. Data:

From the point of view of electrical physics, data and voice are both modulations of the same energy flow, but in the past the parameters of an electrical communications circuit could vary widely enough to profoundly affect the economics of transmission. Also, while data can be made to mimic voice characteristics and

be transmitted over voice lines, such data flows can be detected, and must be handled carefully so as not to disrupt the switching systems. (1)

On the other hand, voice converted into digitized signals by computer techniques becomes totally invisible in the bitstream. Therefore, in the future it is expected that the distinctions between voice and data circuits may disappear. (2)

The present separation of voice and data traffic is driven by economics more than by technology. The voice networks' inherent design and its pricing structure are based on an average overhead which covers connection costs and typical holding times for a

(1) Hence, low-speed modems may not be interchangeable between national public networks. This causes a certain level of inconvenience for the users of portable terminals, and has been cited by PTTs as a reason to prevent arbitrary data connections to the network.

(2) The distinction between analog and digital transmission has been muddied by the new technologies. All telecommunications using electromagnetic energy, whether by wire pair, via radio beams, or on light waves, are modulated and therefore must be termed "analog"--even if these waves carry only a digital bitstream. Since the demise of Morse telegraphy, DC pulses are no longer transmitted long distances without some form of modulation. On the other hand, with the rapid progress towards digitizing all signals--voice or data--in order to take similar advantage of efficient utilization of computer switching and signal enhancement techniques, all links will also be digital, as well as analog. [See, Davies, Donald W., and Derek L. A. Barber, Communications Networks for Computers, New York: Wiley, 1973, chapter 5, which indicates the technical commonality of analog and digital transmission on modern networks.] Not only can digital voice be merged into the digital data or video bitstream, but the network is a processor, too. Codes are converted, routing and content may be altered via on-line "microprogramming," and, in essence, the network becomes a virtual extension of the host computer. The discussion of "record" vs. "voice" carriage, may then become in many applications one of mere semantics.

circuit. This pricing system is thus unsuited to either very short messages or data bursts (overhead too high) or for long messages (charges per unit of connect time too high). The development of digital logic, and the low cost of microprocessors replacing the minicomputers which formally functioned as "front-ends" for communications to host computers, has begun to blur the lines between the use of data, telegraph, and voice circuits for computer communications. Furthermore, it is possible that digitized voice and data traffic may be optimally handled in a single mixed bitstream, particularly in expanded corporate telecommunications networks which will flow over national boundaries.

Any regulations applying separately to those flows, would then require the applications of some form of content analysis. Such techniques of government review of the content of the flow raise even more dangerous issues of invasion of communications privacy than those frequently raised regarding trans-border access to personal data files.

Simply stated, in the proximate future, the only method of determining whether data is being transported across national boundaries in contravention of some national restrictions will be some form of wiretapping; and for full control, that wiretapping will have to be on a gross scale covering all trans-national telecommunications traffic.

2.2 Protocols, Cryptography and Interconnection:

In the discussion of international protocols one notes a frequently expressed desire that data flows be transparent as to content and form, for restrictions can undermine any engineering effort either to innovate or to propagate universal standards of transmission and network interconnection.

But, protocols can also bias choices of hardware. It has been suggested that the use of microcode for interface between "intelligent terminals" and high-level datalinks could constrain manufacturers. Such microcode in computer programs is necessary, however, for the error-correction and cryptographic functions of high-speed data transmission, as well as for other control operations. (1) Another example has been the rather slow merger of Telex (or TWX) and computer data transmission technologies.

(1) These concerns have been voiced in discussions of the Data encryption Standard being promulgated by the U. S. National Bureau of Standards, and the System Network Architecture concept of IBM. See Solomon, Richard J., Mini-Micro Systems, February, 1978, pp. 22-6, Computer Security Newsletter, (Computer Security Institute, Northboro, Mass.), Sept/Oct 1977 and Nov/Dec 1977; and Datamation, March 1976, pp.164-5.

(2) The worldwide standard message system, is poorly adapted to the computer age for a number of technical reasons: slow speeds; no error-correction codes; limited character sets; and general lack of compatibility with data processing technology. The North American TWX and Telex systems were interconnected only by governmental fiat, and then only via a store-and-forward computer system with little flexibility. This was a case of poor coordination, made more extreme since the systems were implemented or modernized in the early 1960's, yet did not anticipate the potential of computer-communications.

(2) So issues of standards are fraught with possibilities for restricting data flow. And even if conversion becomes relatively easy with microprocessors, that does add to the cost and complexities. (1) Among the conversions made relatively cheap by the development of microprocessors is encryption. (2) Some kinds of data communication are quite incompatible with attempts to regulate encryption. In a packet switched international network the individual packets are relatively meaningless and travel through the system in random routes. Any attempt by one country to restrict the code that was allowed to pass through its nodes would be unenforceable, or if an attempt was made to enforce it, would prevent the operation of the packet net in that country. Thus from a technical point of view, freedom of encryption has to be allowed on such a net.

From a policy point of view there are many advantages, as well as some disadvantages that follow from that fact. With recent development of one-way codes it is possible to send a bit stream that is virtually undecipherable unless one has the key. (3)

(1) Interconnection of communication lines has always required a large array of technical parameters to be normalized. For voice, lines have had to be buffered and interoffice signalling made compatible with each switch and with certain line characteristics. Data transmission over these networks had to take into account specific engineering parameters which were intended to economically enhance voice message traffic. However the potential of modern of all-digital networks is that they may transform the balance of such compromises. Network design could then become easier for innovative services in the future.

(2) For further discussion of encryption issues see Section 6.4 below.

(3) Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection", Science, vol. 197, pp.438-440; Martin Gardner, "Mathematical Games: A New Kind of Cipher That Would Take Millions of Years to Break," Scientific American Richard J. Solomon, "The Encryption Controversy", Mini-Micro Systems, February, 1978, pp. 22-26.

That permits virtually absolute privacy or security of the data transmitted, at least from the point of view of the parties possessing the code.

Others may worry that included in this technologically secured data may be information infringing someone else's privacy or property. This dilemma makes clear that technical security alone is but part of the problem. Technical security of data is achievable at a price, (1) but legal and moral considerations enter into the decision as to whose security or privacy to protect by infringing someone elses.

As always, the choice of technical solutions may be influenced by political considerations. For example, in North America, anti-trust measures have played a definitive part in structuring various voice and message services; while in Europe, a major consideration has been the protection of communications revenue. The addition of content restrictions on trans-border communications would add another considerable level of magnitude to the problems already extant in international telecommunications engineering.

(1) Cf. J. Martin, Security, Accuracy and Privacy in Computer Systems, Englewood Cliffs, N.J.: Prentice Hall, 1973. Lance J. Hoffman, Modern Methods for Computer Security and Privacy, Englewood Cliffs, N.J. Prentice Hall, 1977.

3. CAPACITY PLANNING

3.1 Physical Plant

A second area in which international agreements, and also international organization are necessary is the planning and organizing the physical facilities over which transborder telecommunications flow. The problems, even between contiguous countries, are significant, but they are larger for intercontinental communications via cables or satellites.

3.1.1 Cables vs. satellites.

International capacity planning has been effectively carried out in the past by the carriers themselves with little outside interference. International traffic has been profitable so the PTTs were generally willing to make the investments necessary to catch up with demand. Cables were laid by international consortia, the fiction was maintained that ownership of the circuit was divided at the midpoint; payment arrangements were worked out by the carriers among themselves.

With the coming of satellites, the non-technical planning problems became more complex. Decisions had to be made about the balance of investment and traffic between satellite and cable facilities. These are put in place, owned, and administered in different ways, with the result that the division of investment and traffic affects different interests differently. The service

the two modes provide is not identical. For example, cables are laid along the heaviest traffic routes and may serve them well. However, places off those routes could be served in the cable era only by indirect routing through transit nodes. With satellites all points on one half of the earth are equally linkable. The World Cup matches in Buenos Aires could be seen in North Africa without going through New York and London.

Security considerations also enter. Redundancy of systems provides insurance in either natural or man-made disasters. This consideration may lead to having facilities that are otherwise less economic than the alternative and arbitrarily routing some proportion of traffic over each system. In the light of security considerations, allowing traffic to go either over cables or satellites, whichever is cheaper, is not necessarily sound.

In the United States, the problem of choice is made still more complicated by regulatory differences between the alternatives. In most countries the half-circuit from the satellite to the ground link, and the ground link itself, is owned by the same organization that owns the cable, namely the PTT. In the United States one company, Comsat, owns the half-circuit from the satellite, ownership of the earth station itself is shared, and the carriers (AT & T and the international record carriers) own the cable. Since the FCC's rate regulations are based on rate of return on investment, it makes a considerable difference to the companies whether investment is made in cable or satellite

facilities. It is to the carriers advantage to make the case for cable use.

The inadequacy of the present arrangements for capacity planning was brought home forcibly by the TAT-7 case. The American carriers and their CEPT counterparts in Europe, after a long negotiation, arrived at an agreement for a new trans-Atlantic cable. It would be fair to say that most of the push for this scheme came from the American side, and that the European partners were in some instances persuaded to go along with the plan. In any case, the partners put a rather large amount of time and money into working out the arrangements. When all was concluded and the agreements reached, the American carriers submitted the proposal to the FCC which turned it down on the grounds that satellite circuits could meet the demand more economically.

The economics are complicated and cannot be judged here. Even if the FCC is right in that judgment, however, it is clear that the procedure is an unfair one to the European partners. They in each case represent their governments, and when they reach an agreement it is an official one. The American carriers, however, are private firms and the agreements that they reach have no binding effect upon the government. Nor is the government ready to give any kind of declaratory judgment in advance. The FCC acts on fully worked out applications brought to it. It is not a planning body to guide the private carriers in their program

development.

The situation is unsatisfactory. The mismatch can be corrected only by legislation in the USA. Other nations have a distinct and legitimate interest in asking for and influencing such legislation. OECD would be a proper forum in which to explore what sorts of international institutions would be appropriate for international facilities planning.

3.1.2 Volume

It is worth noting that the growth rate in demand for data communications is quite different between countries, and that the expectations of planners as to the likely rates of growth are even more different. Exchange of information, multinational studies, and study groups may help in harmonizing the expectations on the basis of which capacity planning takes place. ITU, OECD, the European Community and other international public and private organizations have played an important role in producing shared understanding.

At the same time, it must be recognized that the differences in expectations are at least as much differences in intentions as they are differences in perceptions. Large scale expansion of international data communication implies priorities in investment and changes in policies which are seen differently in different countries. Countries differ in their willingness to import computing and data handling equipment, to allocate investment

funds to long-lines vs. local service, to allow the growth of private enterprise in interconnected value-added services, and to allow users to experiment with their own interconnected terminal facilities. The rate of expansion of data communication depends on liberality in such matters, so it is not just a difference in forecast, but a difference in policy that underlies different expectations as to the likely rate of growth, and therefore in what must be planned for.

3.1.3 Direct satellite links

Perhaps the most radical change likely to occur sometimes in the next decade or two in international data links is the emergence of direct satellite services (such as the US domestic Satellite Business System plan) that would connect small rooftop antennas without going through the domestic terrestrial system at all. No such system is currently up for consideration internationally. However, if that is as economical for some uses as it seems likely to be, no country interested in maintaining its own productivity will be able to flatly reject the development of such systems just because they will cause drastic changes for the existing communications institutions. (1) We have generally assumed for the near future that most international data communication in areas as densely populated as

(1) "Ainsi le satellite rendra possible l'émission individuelle de telecommunications. Face à ces possibilités, la protection du monopole ne reposera plus que sur des armes juridiques, donc fragiles et temporaires." Nora, op. cit., p. 24.

Europe will continue to travel over public switched services or public leased lines of the domestic carriers. However, a growing part of the international traffic may be expected to operate over circuits that make no use whatever of the domestic carrier's facilities, but simply go from the sender's earth station to the international satellite and down to the receiver's earth station.

To the extent that such circuits come into use, international facilities planning consists of planning the co-operative international satellite system, be it Intelsat or something else for particular regions in the future.

Intelsat has been a great success. Few international organizations work as well. It has not only operated without political rancor, but it has also been a financial success. Its use has grown steadily, its rates are falling, it is moving forward technologically. Intended primarily for intercontinental communication, it is now providing links for domestic service in 17 countries too. (1)

The success of Intelsat in the '60s and '70s, however, does not guarantee that it will meet the problems of the '80s and '90s. That depends upon political decisions. There is every reason to

(1) Algeria was the first. By use of an Intelsat transponder it was possible to link several Sahilian cities in the interior with the capital, bypassing a large investment in microwave facilities. Several other developing countries have in a similar way jumped years of terrestrial system development by going directly to satellite links, which (except in the Indonesian case) were Intelsat.

believe that the most economical way of providing added long distance international communication will be by satellite links using large multinational space platforms. Indeed the current technical literature contains frequent discussions about future switchboards in the sky. There seem to be considerable economies of scale in satellite systems and little economic justification for having numerous national satellites. Thus there is a clear function for Intelsat or regional satellite organizations to provide direct links to ground stations from high powered satellites. It remains an unanswered political question how rapidly and freely Intelsat will be allowed to move into that activity, or what other kinds of competing entities there will be. These are issues that will enter the agenda of various international organizations during the next decade.

3.2 Tariffs for international data communication

If, as we have suggested, there is much uncertainty about how rapidly the institutions for international data communication will be funded in different countries and allowed to grow, it is in part because of the rate structures that will be imposed. Tariffs constitute important institutional and political determinants of the use of transborder data facilities.

For the most part, their rate setting for transborder data flows involves the same familiar problems as rate setting for international voice telephony and international leased lines. In

each case the rates for the two domestic legs of the transmission are set by each country according to its policies, though a major effort is made by the carriers to negotiate rates that will be roughly the same in each direction. In all those situations there is an issue as to whether tariffs should reflect carrier costs or whether they should reflect the value of the service to the consumer, i.e. what the traffic will bear. In most countries the latter is the policy, and international rates tend to be high compared to domestic rates. In the USA, because of a preference for promotion of competition, the FCC has been pressing toward rates more closely aligned with true costs. (1) In most countries where the carrier is a government monopoly, the policy is to earn a surplus on sophisticated services where that can be done, so as to use the revenue to maintain the necessary public services that lose money, such as postal service or rural telephony. In such government monopoly systems too, the rates are often set largely by the carrier itself, and so there is a strong motivation not to allow new services to force old services into the red; thus telex is apt to be protected from the rapid influx of cheap time-sharing mailbox systems.

The question before us in this paper is not which policies are wise or economically desirable, but whether there is any need for co-ordination or harmonization of these policies internationally

(1) Any other arrangement leaves pockets of high return and other pockets of low return or even loss, thus inviting cream skimming competition in the high return areas.

to any greater degree than is now the practice. For leased lines or switched circuits there is no obvious case for greater co-ordination. User and vendors who have an interest in the rapid development of data communication can make a strong case that many countries are setting rates at unreasonable levels which discourage progress. It is, however, a domestic matter, and no special international problem is created by the fact that data communication rates are high in one country and low in another.

While that is so for rates on private lines or on dial-up switched circuits, international packet nets are another matter. Rate setting for packet networks present some new problems since traffic over the net follow random routes. There is no telling what countries the packets that make up a message have been through. PTTs might conceivably charge different amounts per kilometer within their territory for the leased lines that the packet net requires. As long as rates are not volume-sensitive then there is no problem to that. However, for public packet nets, or if the SWIFT precedent continues to be followed, for private nets too, the amounts charged users per packet could not be a function of the countries traversed. That means that the co-operating carriers would have to find a new system both for division of the revenue and for charging. There are many possibilities. Revenue could be divided according to the volume at input or output, disregarding the nodes traversed. Or it could be a function of the kilometers of route within the country -- at least for terrestrial, though not for satellite systems. Or

it could be a function of investment in the system. Or it could be some complex function of all of these and other considerations. What a particular user is charged for a packet, in principle may differ from country to country. However, there is the usual problem that if rates in two directions on a single route are different, people will find ways to originate traffic at the cheaper end. Also, unless the added charge at one node is simply a tax or surcharge, it becomes part of the total revenue and presumably largely benefits other countries with which the earnings are shared.

None of these problems are insoluble or even extraordinarily difficult, but they are new, and being new they do call for continuing international discussion until they are worked out. They are, of course, now under active discussion among the carriers, for international packet nets are rapidly coming into active use.

The most important recent decision made regarding them was on SWIFT, the interbank clearance network that was established last year. At the time of its planning, the banks calculated what they would save by creating a private line packet network rather than using mostly telex as they had in the past to report the daily clearances. Shortly before they were to go into operation, however, the CEPT carriers decided to deny them service at the established private line rates, and to charge them, instead, a volume-sensitive tariff, the cost of which would be intermediate

between what telex had cost them and what private lines would have cost them. The PTTs were unwilling to accept such a large loss of revenue. Furthermore, the SWIFT decision was generally viewed as a precedent for what should be done with regard to any future requests to establish dedicated packet nets.

The banks and other private line users have vigorously protested this decision. It is not for us here to consider the merits of the case, but only what is at issue. The proponents of private lines argue that such facilities permit large users to develop technologically sophisticated communications systems and thus aid productivity and economy. The opponents of private lines argue that the economically powerful large users are economizing on their communications costs at the expense of the PTTs and thus at the expense of the small user who must pay more of the total. Both arguments are in part right and in part wrong.

It is true that the abolition of fixed rate leased lines and the introduction of volume sensistive prices will make it less profitable for large users to develop high speed multiplexed communications networks. However, the effect of a change to volume sensitive rates is not likely to be that the big users spend less on communications technology and pay more to the PTTs. The effect is likely to be that they invest in different kinds of communications technologies so as to keep their bills low. With fixed rates for leased lines, the technologies that pay are ones for pushing more traffic through the same circuit. With volume

sensitive rates, the technologies that pay will be ones for data compression and other means that allow the same information to be conveyed with less bits of traffic. Distributed computer systems will play a particularly important part in such a situation. Data will be processed extensively locally on minicomputers so that only the heart of the data has to go onto the telecommunications lines. In short, volume sensitive rates are likely to end up being good for the computer industry, less good for telecommunications equipment manufacturers, and no better for the carriers who will carry less traffic at higher returns per bit. For the large users the costs perhaps end up as no different once they have gone through the trauma of a major change.

These issues are ones that are already under active discussion in the community of carriers and telecommunications users. Continuation of the discussion in ways that will lead to greater clarity and to an evironment of confidence about the stability of the rules of the game is important to the development of data communications.

4. TRANSBORDER MOVEMENTS OF NON-PERSONAL DATA

Commercial security is a priceable product. It is, as we noted above in Section 1.3, significantly different from the personal privacy of human third parties who may need government protection to secure themselves against intrusions by others. Private citizens are often weak and easily victimized. That is not the situation of business enterprises that choose to use automated files. Such firms may be presumed to be capable of making a rational choice about the level of security that they require, given that they need to pay for it.

As a Secretariat Note on the former OECD Data Bank Panel said:

> Protective measures are generally expensive, and increase the costs of the processing and transmission of data.

We would argue that, in the absence of externalities, no standard of security of computer files need be imposed on enterprises. Unless there are externalities, each enterprise should be allowed to undertake to buy as much or as little security for its records as it wishes.

Two main externalities from data transactions come easily to mind. One of these, invasions of the privacy of third parties, has been widely discussed elsewhere. The other common externality is the consequences of tampering with the records of customers and suppliers, i.e. fraud against them.

In the latter case a third party may suffer financial loss from the carelessness of those who allow files to be mishandled Suppose, for example, that a bank takes the risk of inadequately securing its records; that could lead to an invasion of the privacy of its depositors or also to stealing from their accounts. We take it as not self-evidently a matter of public concern to protect the bank itself from its imprudence; national policies will differ on that matter. It is much more clearly a matter of public concern to protect the depositors who may be the innocent victims. They can be protected in a variety of ways. A bank can buy insurance, or it can choose to reduce its insurance costs by investing in data security. Some governments would regard that choice as a matter for the bank itself to decide; such governments would limit themselves to requiring that the bank be accountable to its depositors for their funds. Other governments, however, will feel a responsibility for determining that the method of protection chosen by the bank be an adequate one, and will specify bank practices to be used to protect the depositors.

So with governments differing widely in how they see their role, it seems impracticable to expect effective substantive standards to be set by international agreement. Government policies and standards on such matters as the method to be used for protecting bank customers will be more easily and more intelligently set by domestic than by intergovernmental processes. OECD and other international organizations can serve as forums for the exchange

of experience about these difficult questions in a period of rapid change. Also they can serve as forums for the ironing out of agreements to take cognizance of each others laws. Each country could adopt a law making it domestically illegal to attempt to violate certain foreign laws by telecommunication from its own terrain. An agreement for such comity does not require agreement on the full substance of standards. It is not clear that, for non-personal data, anything is gained by seeking to establish any more detailed standards than that.

The question of the usefulness of protection standards for non-personal data is raised in Section 18 of the Secretariat note. It observes that logs of

> "access records to scientific and technical information networks, which are kept for billing purposes, might be misused for monitoring of research activities of competing firms. Therefore, unauthorized access to the enquiry records in information systems might compromise the 'privacy' or proprietary rights of industrial firms or research organizations."

By the criteria we have laid out, however, such protection of industrial firms and research organizations does not seem an appropriate objective for international concern. If such institutions believe it important to keep logs of their enquiries secret, and if they distrust data base managers, they are perfectly capable of protecting themselves at a price. They have

several options, including:

> obtaining their data from several competing data sources so no-one has a consolidated record of their requests;
>
> filing their enquiries for data under various separate and disguised accounts;
>
> blanketing their enquiries in the chaff of additional meaningless enquiries, etc.

All these strategems cost money, but the charge is assessed on those who want the protection; imposing standards, on the other hand, levies the charges on others who do not share the need.

Such considerations militate against compulsory minimum standards for non-personal data bases where no weak third parties are jeopardized Even in such cases, in which setting compulsory standards would be overprotection, governments and international organizations have a role in education and in clarification of these little understood issues. Symposia and publications can help enterprises and institutions become more aware of what the novel problems are and what solutions are available. OECD has already played a very significant role in bringing these new issues into the limelight. (1) In the chart we presented in the

---

(1) While the principle may be accepted that restrictive controls are needed only in the presence of externalities that hurt weak victims, the lines are not always easy to draw.

The Secretariat Note mentions the difficulties of separating personal from non-personal data. Access logs, for example, constitute personal files too though they arise from operations on non-personal data. Insofar as these records constitute abusable records on citizens, they are back in the domain of personal records, subject to appropriate concerns. This problem is exemplified by the familiar practice of selling of mailing lists. A list of those who had accessed data on a given subject

introduction, noted that for data that does not deal with real persons individual protective action by which institutions would secure their own data. But institutions too, as well as real persons, face problems concerning fraud contract enforcement, intellectual property and payments. We turn now to consider the requirements for international cooperation in those areas where law enforcement is vital.

---

would be useful to advertisers with a similar product. Such use of a mailing list can be a useful service to those on it -- bringing things that they are interested in to their attention -- or it can be a nuisance. Different international jurisdictions may see that balance differently, but insofar as personal data on database users is what is being used, all would probably agree that it is an appropriate matter for public concern.

Thus while data bases may generate mixes of both personal and non-personal data, it would seem to be the former that are generally the major subjects for regulations that set security standards.

5. CONTROLLING COMPUTER FRAUD

One problem that may emerge with the spread of international computer networks is that of illegal activities conducted at a distance, outside of the effective control of domestic authorities. An image has been created by the popular press of computer criminals working in their basements with sophisticated electronics, connected to telephone lines, and making distant computers enrich bank accounts, steal data, or manipulate information. This image has been further delineated by the revelation, at least in North America where the telephone system in the past has used in-band signalling almost exclusively, that computerized devices can be used to dial free telephone calls. It has also been fostered by anxiety about the growth of tellerless banking. (1)

---

(1) Cf. Ralph Blumenthal, "Electronic Fraud Accompanies Tellerless Banking", New York Times, Sunday, March 26, 1978, p. 1. The story starts with characteristic alarm, which when it gets to the facts shrinks to considerably more modest proportions. "Electronic fund transfers," it begins, "which have begun revolutionizing consumer banking with automatic tellers and 24-hour cash-dispensers, have also produced an unwanted breakthrough -- electronic fraud and embezzlement.... Thousands of such frauds have already occurred in the United States and abroad." Then it goes on: "However, so far, apart from several sensational cases of corporate computer fraud involving many millions of dollars, almost all the cases touching on the consumer involves the more limited theft and misuse of chash dispenser cards.... Overall, compared with the millions of customers who line up uneventfully nights and weekends to use the convenience cash dispensers the incidence of victimization remains miniscule. While some experts are concerned, banking officials do not appear alarmed....

One estimate puts the total nationwide loss at $2.5 million last year -- equal to about 10 perdent of the far more spectacular

While computer crime is not to be minimized, we should realize how difficult it is to make a computer do what a programmer wants it to do, even with access to proper documentation. It is even more difficult to mount an unauthorized attack from the outside that would successfully penetrate a complex system. Unauthorized access requires either the patience of a saint, or economic backing sufficient to unravel the intricacies of a computer's programming web. Thus crimes in which computer manipulation is central, when they do occur are likely to be manipulation by insiders or by quite sophisticated organizations like governments, rather than trickery by mere clever outsiders. In the cases to date, the evidence has shown that there has been some insider involved. (1) Those crimes may be of relatively large magnitude, even if uncommon.

Several possibilities for securing banking systems and other holders of entrusted wealth against remote "tampering" may be more feasible than trying to achieve a multi-national definition of a criminal code.

---

conventional bank robbery losses."

With 7729 cash dispensing machines installed in the US, this amounts to about $325 per machine per annum. The examples of crime described all involve misappropriation of the customer's card or insider action.

(1) Donn Parker, Crime By Computer, New York: Scribners, 1976, describes a host of real scenarios where criminals managed to utilize flaws in programming or physical security to penetrate computer systems. None of the protaganists were "naive" in any sense of the word, but the victims often fell into that class!

(1) Secure encryption of transmission. (1)

(2) Agreement on origin identification labels, secure against tampering, and capable of standing up in national courts.

(3) Increasing the liability of fiduciary institutions for stolen or distorted data that they hold. Banks, for example, if properly regulated, should not escape responsibility if their electronic funds transfer systems (EFTS) are manipulated from outside the borders. With liability thus impinging on them, the industry would have to acknowledge the true costs of data communications, and design proper safeguards or be penalized.

Monitoring of data flows by external agencies is likely to be no more effective for law enforcement than would be testing a river's estuary to prevent water pollution: better to control at the source by improving banking practice.

While evolving computer technology coupled with the new data networks will cause novel problems to those in finance responsible for the secure custody of funds, the headaches will not be of previously unknown kinds. The patterns of fund handling from the past may speed up, but the management of funds

---

(1) Cf. Sections 2.2 above and 6.4 below.

will still be best done by vigilant bankers, encouraged to be vigilent by a system of responsibility. The best way to handle the new elements introduced by EFTS is to educate those who already understand their industries best in the new techniques of data communications.

The reader will recall that in a chart in the Introduction we listed some areas of regulation and some appropriate types of international action. With regard to data regulation for preventing fraud, however, we labelled the situation as too complex for a one word description. The row in the chart was as follows:

Area of regulation	Type of international action	
	For data on Real Persons	For data on Legal Persons
Data regulation for preventing fraud	?	Comity

What we now present as appropriate areas for international action are a couple of specific data rules: to allow encryption and set standards for origin identification labels. (1) Computer labelling of origins of messages may seem like a purely technical matter, but it has substantial significance as an appropriate compromise between lack of control of fraud on the one hand and

(1) In the design of most telephone systems no provision was made for cognizance of the origin of calls received because the information was not needed for billing purposes. This has proved a major error from the viewpoint of law enforcement. That mistake need not be repeated with data networks.

censorship on the other. Security of data, like the sealing of envelopes, protects lawbreakers as well as law abiding persons. That is one of the costs of privacy. If, however, it is felt that there must be some way of keeping track of who is transmitting potentially improper messages, the obvious compromise is to keep track of some external label on the traffic (analogous to the outside of the envelope). If that is to be required (perhaps only of traffic of certain kinds of institutions such as banks), then there must be agreement on the form of the identification label, and standards for it that would serve to make it relatively free from tampering, and capable of standing up in national courts.

Primarily, prosecution of fraud depends upon domestic law enforcement in various countries and therfore on comity in legal relations between countries. In particular where the victims may be individuals who lack the resources to bring civil suits in foreign courts, a strong case could be made for international agreements to help protect individuals from vicitimization. So we identify this area of fraud -- along with the protection of the privacy of individuals -- as one that may well require further study of what protections are needed. In particular it would be well for OECD to monitor what happens as computer networks spread, and to keep an open mind as to what international actions may be needed.

For the moment a clear requirement exist for the development of comity between nations in law enforcement against fraud by data communication. The word "comity" is one we have used several times but not explained. We turn now to explain it and its role in law enforcement.

6. ENFORCEMENT

6.1 Criteria for Action:

Several criteria may guide us in evaluating proposals for international agreements. One of these is to minimize international action. Even if it be concluded that social welfare will be served by action, we postulate that in a world of nations, action should be left to each individual nation, unless there is some compelling need for co-ordination.

Another criterion is that most international agreements should sustain rather than supplant domestic laws. Some international agreements, such as those setting engineering standards, constitute a kind of international legislation (even if they have to be nationally ratified) in that they reach a fixed conclusion as to the content of what should be done. Other international agreements, such as copyright conventions, in general just provide a mechanism by which laws adopted in different countries can be made effective against evasion abroad. Under the principle of minimizing international action, preference should be given to agreements that sustain domestic laws, if that will do the job.

Aside from some rather important engineering standards, it is hard to think of areas in which international co-operation for transborder data flows requires substantive uniformity of practice among the countries involved. For the rest, the kind of co-operation that seems to be required is agreements to support

the domestic law of different countries against attempts to evade those laws by operations from a distance carried on across a border. An essential condition for this kind of agreement is that all parties to it regard a particular genus of action as illegal. A country will not generally be willing to help another country prosecute an action which the first country regards as proper or even laudatory. For example, a country with free press will generally not be willing to help a dictatorship prosecute its dissidents for publishing, nor will a country that bars racial discrimination help another enforce laws suppressessing a minority. While there must be agreement by both countries on the need to forbid the general category of activity, the details are left to each to carry out in its own way.

6.2 Areas for International Action:

One can suggest a number of areas, all of them concerning law or contract enforcement, in which the kind of agreement that we are here describing -- without specific international standards -- might well be considered. In particular:

1. Locus of liability: If in an illegal activity or contractual liability, data is physically located in one country but accessed from another, where has the offense taken place and who prosecutes or sues? The problem will become more complex when, in the 1980's, we enter an era of distributed data bases. Analogous problems have been met by courts in the case of mails and telephone, (1) but in some on-line computer systems such as EFTS they become so

(1) Where, for example, is a contract made, that has been sealed orally in an international phone call. That old problem that courts have dealt with since the turn of the Century is identical to what arises with data networks.

critical to effective law enforcement that formal legal arrangements among countries may be desirable.

2. Computer fraud: While, as we have just noted, this is much less of a problem than some popular journalistic treatments suggest, computer fraud is a problem. To help meet it, countries could agree to each incorporate into its own domestic law a provision making it illegal to knowingly access a computer in another country for the purpose of carrying on certain specific activities that are illegal in that remote country. Among kinds of activities that might be listed are such ones as seeking personal information from a data base to which the receiver is not entitled by the laws of the host country, withdrawing funds from an account to which he is not entitled under the laws of the host country, or debiting the account of another person without authorization under the laws of the host country.

3. Illegal use of computer facilities at a distance: Similarly, a convention could bind countries to each enact provisions making it illegal to use computer facilities in a foreign country by telecommunications, without legal access in the foreign country. The purpose of this provision is to enable facility owners to enforce their usage charges and to prevent illicit access to private facilities. However, it could be argued that the computer facility should exercise due care if it is to be protected. That opens up to discussion the question of what constitutes due care.

4. Contract enforcement: To facilitate the enforcement of contractual agreements between computer or file owners, on the one hand, and their users abroad, countries could adopt laws to give recognition to liabilities incurred under such agreements.

5. Relationships of public trust: There are certain institutions that have a special relationship of public responsibility to their customers, of a character that is recognized in almost all countries. For example, banks have special fiduciary relations with their customers; doctors have certain obligations to their patients; airlines have certain obligations to travellers. These go beyond the principle of caveat emptor under which the vendor is obliged only insofar as he has explicitly contracted. In some such situations of public trust there could be evasions based upon transborder telecommunications operations. A frequently cited example is that of data sanctuaries for personal data that it would be illegal to use domestically. Another example would be the setting up of quack medical treatment by telecommunications.

When, as, and if any such problem becomes significant, it would be appropriate for governments to provide by convention for the common maintenance of the standards of public trust that they share. Since these standards are specific to particular areas of activity, there is no way of reaching general conventions or standards in advance. Agreements on specifics will have to wait until an abuse begins to appear, and its character and significance can be assessed. The two fields in which causes for concern have begun to arise, and which might be fruitfully discussed in the near future are privacy and electronic funds tranfers.

6.3 Difficulties of enforcement:

The kinds of regulations that we have just listed are relatively enforceable because they address a systematic pattern of illegal behavior of a particular kind, and not just the physical flow of code on transborder circuits. If someone has not paid his computing bills, or has used a computer without permission, or has fraudulently manipulated an account, there may be many kinds of evidence of that misbehavior. The procedures for law enforcement in such cases are the normal procedures of civil or criminal law. On the other hand, some proposals that have been made, which would regulate transborder data-flows in general can be faulted as unrelated to particular evils. To enforce a requirement that no illegal data be transmitted, for example, would require monitoring the content that is represented by the bits flowing over the circuits. It would require cognizance by the authorities of what those bits represented. Such proposals are virtually unenforcable. Attempts to restrict data that is flowing across borders, by specific content or format might have worked (albeit badly) in the 1960's but will surely fall under

the technology of the 1980's. It may be evaded by users in several ways:

(1) If economic and political risks justify it, the user can circumvent the regulation by skilled programming or manipulation of hardware, by ignoring the regulations, or by making proof before a court of law either too expensive to try or virtually impossible. The complexity of programs and cyphers supports the evader.

(2) If the regulations cannot be circumvented, the user may move his data processing business and ancillary activities somewhere else. Those countries that avoid excessive regulation will attract business, especially those highly mobile businesses whose main assets are information.

(3) A combination of the above--that is, there may be a mere pro forma meeting of the trans-border restrictions, while the actual data processing activity is performed elsewhere.

Such strategies are increasingly difficult to contain in an era of all-digital systems and distributed computing.

Relevant data may from the start be located abroad in places where it is legal, and read where its use is not legal. If the data originates where its use is not legal, governments may try to disallow its export to data sanctuaries, but only with limited success. Data that is barred from electronic delivery can go

through the mails, and even electronic delivery cannot be effectively monitored. A clever evader can send any data abroad that he wishes with small chance of detection. A large organization will be inhibited in its systematic procedures by awareness of regulations, because it has so much at stake if it is caught. The rules, therefore, can have some statistical effect, but not more. Experience with prohibitions on export of unlicensed personal data is that such rules are hard to enforce.

Furthermore, attempts at regulation often have effects quite different from those that are anticipated. For example, copyright and patent regulations require the revealing of secrets, so computer software owners sometimes prefer secrecy to legal protection, and may even choose not to use the protections that the regulations make available. Another unanticipated consequence of attempts to police data strictly can be to drive data-using businesses to locations where standards of regulation are at a minimum, thus in the end lowering rather than raising the degree of control.

6.4 Encryption:

A development that is making control of the content of the bit stream virtually impossible is the progress of the art of encryption. Encryption is useful for two sets of purposes; it is used to protect privacy and also to aid national security. However, these objectives sometimes come into conflict. Some governments concerned about national security, prohibit

encryption by private communicators, and indeed sometimes justify this action as preventing violation of the country's privacy regulations.

Such attempts by regulation to increase security of non-personal data bases may have just the opposite effect. To regulate files requires knowing what is in them. If they are thoroughly encrypted in high quality code, it becomes impossible for the regulators to know what is in them. It is therefore tempting for regulators to prohibit such encryption. But this eliminates the use of one of the best protections of privacy.

Recent technological developments (such as one-way codes) have made encryption easier, cheaper, and more secure than ever before. It seems unlikely now that practical codes can be broken at reasonable cost. (1) Many devices that were practical for controlling of communications in the case of hard copy print output,, are impractical for computer data. In the absence of the solid evidence provided by the physical written sheet, and without the point of leverage for enforcement that the printing press provides, it is far from clear what governments can do. Attempts to regulate such things will result in vast measures of government intrusion into operations, with only a statistical measure of success, and widespread violations. The convention that many governments adopted in the telegraph age of allowing use of cyphers only if they are deposited with the authorities is

(1) See section 2.2 above

quite unenforceable on data networks.

6.5 A Look Into the future:

Once text is loosed within a computer network, outside of its owner's files, it is virtually impossible to police it, to know who has used it, how often and when. We must, of course, assume that some persons are motivated to disregard proprietary considerations. Let us consider what options are open to them:

Person A has legitimate access to a proprietary file: person B has read-only access to A's files and copies the document. B transforms its format so that while the content remains the same the bit representation is different; he then purges the original. B lets C read the reformatted text; C copies it and encrypts it and sends it over the network to D; etc. etc. Even if trails are kept of the accesses to A's and B's files, once the text has been transformed there will be no record that the new file is substantively identical in bit pattern it is unrecognizable. Even if a censorious government listens in to what is transmitted, it has no way of reading the encrypted material.

So it seems clear that in computer communications, protection of intellectual property is going to be difficult. At most governments may help vendors to enforce some restrictions on their immediate clients. Governments will undoubtedly differ in the degree to which they choose to support the proprietary interests of data vendors. With the experience of some decades,

perhaps some common practices may emerge. In the short run, however, governments may be expected to adopt varying laws on data theft and on contractual liability. In a fluid and novel situation, in a world of sovereign states, uniformity in such matters is not to be expected.

7. THE BORDERLINE BETWEEN DATA PROCESSING AND TELECOMMUNICATIONS

In various countries an effort is being made by regulatory authorities to distinguish data processing from telecommunications services. Telecommunications are typically a legal monopoly; the computing industry is typically private enterprise. However, as the Secretariat's Note remarks, they "acquire increasingly similar aspects and interpenetrate." To avoid encroachment by private companies on the telecommunications monopoly or encroachment by government into computing, the regulators have tried, without success, to find a logical dividing line between them.

The US experience may be seen as prototypical. The Communications Act of 1934 imposes on the FCC the legal obligation to regulate electrical communication, including the licencing of carriers. With the arrival of remote computing, it became apparent that every computer is potentially a switched telecommunications device. In a stand-alone device communications takes place over inches or feet, but with remote computing even that quantitative distinction between computing and communication vanished. Yet the FCC had neither the desire, nor presumably the authority, to extend its jurisdiction to the large computing industry. So, as a means of continuing to obey the legal injunction on it to regulate communication and still stay out of computing, the Commission invented a distinction, as follows:

> "...Data processing" is the use of a computer for the processing of information as distinguised from circuit or message switching...." "...Hybrid Service' is an offering of service which combines Remote Access data processing and message-switching to form a single integrated service....." "...Hybrid Data Processing Service is a hybrid service offering wherein the message-switching capability is incidental to the data-processing function or purpose...." (1)

If taken as a serious intellectual matter, it is easy to dismiss this classification as absurd. Even as a pragmatic formula it broke down. An increasing number of real world activities fell on the debatable borderlines. So the FCC has sought another formula. The proposed definition of computing is:

> "the use of a computer for the purpose of processing information wherein: (a) the semantic content , or meaning, of input data is in any way transformed, or (b) where the output data constitute a programmed response to input data." (2)

That is no more successful.

If approached quite cold-bloodedly as a device to separate situations that the regulators wish to become involved in from ones they wish to stay out of, then all these discussions of how many angels can stand on the head of a pin are legitimate. However, no one should believe that, if only one thinks clearly enough, out there in nature a separation can be found between electronic communication and computing.

---

(1) (47 CFR 64.702; also see 17 FCC 2d 587 , "First Report")

(2) (Docket no 20828, Notice of Inquiry, July 29, 1976, FC76-745, --FCC--.

It is informative to compare the responses and replies to the FCC by the two principle adversaries, IBM and AT&T. There is remarkable agreement between them.

Says IBM:

> "The parties who have commented express a clear consensus that the definitions proposed by the Commission to distinguish communications common carriage from 'data processing' for regulatory purposes are extremely confusing. ... Most parties agree that this confusion and disagreement result from a flaw in the basic conceptual approach proposed -- the notion that 'data processing' and ' communications' are mutually exclusive and therefore can be defined without overlap." (1)

Says AT&T:

> "We recognize that a confluence of data processing and communication is occurring.... The basis for making regulatory distinctions cannot be that 'communication' and 'data processing' are to be considered 'mutually exclusive activities'.... To do so would place a desire for 'regulatory certainty' before a recognition of the realities of the current state of computer technology." (2)

There also is agreement between them in arguing that the central issue which the FCC should be addressing is not the whill o'the whisp of a scholastic technological distinction, but rather the question of the proper structure of the industry. Even on that

(1) Reply of International Business Machines Corp. Before the Federal Communications Commission, Oct. 17, 1977, pp. 2-3. At another point they repeat: "Definitions should be designed to describe reality. The proposal in the notices instead seeks to mold and thus to alter reality. Virtually all parties to this proceeding agree that the basic assumption... that it is possible to classify processing activities as either communications or data processing based on the nature of the processing performed' -- is unsupportable." Ibid. p. 34.

(2) Comments of American Telephone and Telegraph Co. Before the Federal Communications Commission, June 6, 1977, p. 104.

they are in partial agreement. AT&T argues that it and other regulated communication carriers should be allowed any data processing activity or to supply any equipment that may help it meet "the needs of the user public for more varied and sophisticated communication services." (1)

IBM agrees. It goes further and proposes that "carrier entities would be permitted to engage on an unregulated basis in the provision of all data processing services and equipment." (2) IBM is asking that AT&T be allowed to compete with it in all its activities. (3) The counterpart to this pro-competitive doctrine as stated by IBM is to restrict the regulated monopoly part of AT&T's business to transmission alone; with that AT&T, of course, disagrees.

Thus despite their inevitable differences, these two leading actors in the field both recognize that the attempt to draw a hard line between data processing and telecommunications is an exercise in futility. They both recognize and accept the fact that they are in an era when in many of their activities they will inevitably compete.

(1) Ibid.

(2) Response of International Business Machines Corp. Before the Federal Communications Commission, June 6, 1977, p. 4.

(3) IBM argues that accounting separation of competitive and monopoly activities is all that is needed, not even arms-length subsidiaries.

Indeed, the distinction will become increasingly difficult to draw with the introduction of digital voice and a common bit stream of voice and data. While conversion of the vast telephone plant will take many years, the first major installations are underway. (1) Bell Canada has announced that all new switching installations will be digital with time division switching. Bell Northern has announced the production of an all digital hand set. General Telephone and Electronics is installing all digital exchanges in small rural offices on grounds of economy. Thus a movement towards bit streams in which voice and data are fully merged is upon us. With that, the separation of those parts of the bit stream that are engaged in computation from those parts engaged in moving messages becomes quite impossible.

There are indications that the FCC itself may be having second thoughts about the stress that it has put on the computation/communication distinction in the past, important as it may be for them as a legal fiction. The computer enquiry has been moving very slowly, and conversational comments would suggest a lack of desire to press into what is recognized to be a thankless task.

(1) Use of Digital (PCM) transmission dates back to the early 1960s in exchange area trunks. The first digital PBX's go back to shortly after. but systematic replacement of existing systems by fully digital facilities is only now getting underway.

8. PROPERTY RIGHTS IN ELECTRONIC DATA

8.1 Some Historical Background:

The concept of copyright is rooted in the technology of print. The recognition of a property right in text and the practice of paying royalties, emerged with the printing press. (1) Numerous copies reproduced in one place, made it feasible to identify the source of the copies and how many had been made. The printing plant was a practical place to apply control.

The practice of copyright in Britain, though not the word, began in 1557 when Philip and Mary in an effort to stop seditious and heretical books, limited the right of printing to members of the Stationer's Company, and gave the company the right to search for and seize anything printed contrary to statute or proclamation. Eight years later, the Company, under that power, created a system of copyright for their members. (2) In 1709 the first British Copyright Act for authors was passed.

(1) The English word first appears in 1767 in Blackstone's Commentaries.

> "However, the concept of copyright goes back much further than Blackstone... In effect, though, the right only began to assume importance when the invention of printing made the multiplication of 'copies' of a work infinitely quicker and cheaper then the painstaking products of monkish scribes, as well as appreciably more accurate than the compositions of most professional scriveners."

Ian Parsons, "Copyright and Society," in Asa Briggs, ed., Essays in the History of Publishing, London: Longman, 1974, p. 31.

(2) Ibid, pp. 33f.

For modes of reproduction where such an easy locus of control did not exist, the concept of copyright was not applied. Until quite recently it was not applied to conversation, or speeches, or singing of songs whether in private or in public. It was a specific adaption to a specific technology.

8.1.1 American Copyright Practice:

The landmark case in the United States was White Smith v. Apollo. (1) It denied protection to piano rolls or sound recordings because they were not "writings" in tangible form, readable by a human being.

Many new technologies of communication since 1908 were excluded from protection by that common law concept of copyright. But the motion picture industry the recording industry, and more recently the broadcasting industry have persuaded the US Congress to extend protection to them which the courts had refused. For movies and phonograph records, that extension was reasonable. Like books, they were physical objects produced centrally in multiple copies. However, for of radio, electronic reproduction, and now electrostatic copying, there is no easy way to keep tabs on the numerous reproductions in somewhat variable

(1) 209 US 1 (1908). Cf. also Goldstein v. Calif. 412 US 546 (1973) on sound recordings. Within the context of the protection of writing, it is the form and manner of expression that is protected; the ideas expressed by the author of the copyrighted work are not protected. A typical American statement in the case law of this principle can be found in Becker v Loew's Inc., 133 F 2nd 889 (7th Cir 1943), certiorari denied.

form that can be made in innumerable locations. The analogy is to word of mouth communication in the 18th Century, not to the print shop of that period.

Nonetheless, industries, whose welfare depends upon finding ways to charge for their services, have sought to extend copyright protection under statute law, to the new technologies of computerized data, photocopying, and telereproduction. They grab onto whatever frail reed the existing copyright system may provide rather than turning to the even frailer reed of trying to invent, and to get into legislation some entirely new, as yet undevised system for rewarding the creators of information.

8.1.2 The New US Law:

In the United States, a new Copyright Law was passed in 1976. (1) The main issues concerned new technologies, -- electrostatic copying of printed articles especially. In 1975, it is estimated that 365 billion impressions were made by duplicating machines in the USA. (Predicasts estimate.) Of those, an unknown number reproduced copyrighted material. Publishers believe this is discouraging journal publication; the number of scientific and technical articles published rose from about 106,000 in 1960, to just over 150,000 articles in 1974, or a growth rate of less than 3% per annum. (2)

(1) 17 USC ss. 101.

(2) US National Science Foundation, Statistical Indicators of Scientific and Technical Communication, 1960-1980, (data from

In an effort to cover the new technologies of information the new law changed the basis of American copyright. The crucial clause states that copies are material objects, other than phonorecords,

> fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced or otherwise communicated either directly or with the aid of a machine or device. (P.L. 94-553, ss102a.)

American copyright used to require "publication" to become effective; now the right stems from merely "fixing" the work in some material medium. (1) This was intended to provide copyright for cable television (CATV), electrostatic copiers, and computers. (2) Whether this change has solved any problems or merely exacerbated them is an open question. The new rules in some fields continue to be as often violated as obeyed. Libraries now post a notice telling those who use the copying

---

King Research Inc.), p. 81. That compares with a growth in scientific and technical book titles in the US in the same period from 3379 to 14,442, or a growth rate of 12%. In the Bill, a National Commission on the New Technological Uses of Copyrighted Works (CONTU) was established, to report back to the Congress on the working of the new copyright law. Its report is anticipated in July, 1978.

(1) There used to be in American law, separate common law and statute law concepts of copyright. The common law recognized the specificity of the concept to the nature of the print medium. Statute law extended copyright to various other media. With the new statute, statute law has completely occupied the field.

(2) Although computer programs are not explicitly mentioned in the new law, they are covered by the description of text as "words, numbers, or other verbal or numerical symbols or indicia." Reproduction is allowed under the old "fair use" doctrine which is restated in section 107. Section 108 authorizes libraries (for non-profit purposes) to reproduce single copies of works that would not have been justified under fair use.

machines that they are not authorized to recopy and redistribute the copies, and that the copies are for the scholars personal use, but there is no enforcement. CATV operators pay a fee for a compulsory license to transmit non-local broadcast programs originated by others than the networks; the law does not provide a payment system for material that is cablecast but not picked up from broadcast, so all the difficult questions will come up again when broadband switched networking comes into general use.

The outcome in the United States is likely to be neither equitable law enforcement nor a total sham. Unenforcable laws do not prevent individuals from doing what they want to do under the cover of privacy and corruption, but they do prevent substantial responsible institutions such as corporations and universities from addressing themselves to meeting the public demand where it could get them into trouble. These institutions do not wish to risk large stakes by petty violations. Thus unenforceable laws produce a mix of contempt for law plus some statistical impact that may or may not be desirable.

8.1.3 Comparison to Continental European Practice:

The rest of the world is struggling with the same set of problems, but in a different legal context. Most national copyright laws include under "literary and artistic works", not only text, but also musical works, drawings, photos and motion pictures. The Berne Copyright Convention, first drafted in 1886, and revised seven times till 1971, in particular has made some

effort to keep up with technology, e.g. protecting recording on magnetic tapes. However, only 66 countries adhere to Berne, and its present organization, WIPO (World Intellectual Property Organization). The USA and the USSR do not adhere, nor do many developing countries. After World War II, an attempt was made to establish a convention which those who had not signed Berne could accept. That led to the Universal Copyright Convention of 1952. It has 67 members. That convention puts more emphasis on works being visually perceived. The World Intellectual Property Organization recently published a report on a "model law" for the legal protection of software. It applies to the protection of computer programs, not to the protection of computer data. It does not deal with a number of the problems that arise in distributed computing.

The primary purpose of copyright law, as often declared, particularly in the Angle-Saxon countries, (1) is promotion of science and the arts. In that view, this goal is above the additional purpose of protecting the tangible intellectual labor of the author. The school that sees copyright as a natural right would not necessarily agree.

For the work to merit protection, it must possess some "creative originality." It must reflect the author's own skill, labor, and judgment and must be more than an industrious collection of

(1) For US precedents see Berlin v E.C. Publications Inc., C.A.N.Y. 1964, 329 F. 2nd 541, certiorari denied 85 S. Ct. 46, and others in 17 U.S.C.A. sec. 1.

previously known material already within the public domain. In Continental copyright law (e.g. French and German), but not in British or American, there is a droit moral, that is the right not to have your work distorted or mutilated in reproduction. This is separate from the economic rights of the author. While there have been no cases as yet, the droit moral could apply to a scientist who has changed his views or might want to be meticulous about the exact statement of his thesis.

8.1.4 Summary

It will be difficult to apply some of these concepts to computer data processing or transmission. For the greater part of a century after the introduction of electrical communications, violation of copyright was no more of a problem than other forms of mass-produced counterfeiting; the problem was soluble because the tools were crude enough to give themselves away. A counterfeit, whether of an image or a sound, was worth the risk only where the original was of high value.

Historically, technological violation of copyright first became a problem with recordings, (1) then with copying machines. Before the advent of xerography, little photocopying was done, save at high cost by the photostat process or via microfilm, or on vastly inferior duplicating machines. But, xerography is of

(1) Cf. "Record Pirates: Industry Sings the Blues," New York Times, June 30, 1978, estimating the US volume of illegal recordings at $200,000,000 per year.

the utmost simplicity. So is the use of audio cassette recorders, and so is the use of computers for copying files.

8.2 The Application of Property Concepts to Computer Data.

Virtually all of the legal concepts that we have here introduced can be applied only with difficulty to modern computer applications. Consider the fact that out of a computer can flow an almost infinite variety of slight modifications of the elements of text that are in there. In print publishing any one edition is likely to run to thousands of identical copies. There may be a legal issue as to whether the differences between that edition and some source material is so small as to be a violation or big enough to meet legal requirements, but it is not a question that arises with every single copy separately; it can be resolved in court for an entire edition. Compare that with the output from a computer information bank. The individual items in the data bank such as article titles or chemical formulae or equations may be in the public domain. The organization of them in the data base may be sufficiently distinctive to be a protectable work of genius, though it is never published in raw form. What is published is combinations generated by the user. Is that his property or that of the data base creator? Anyone else coming along giving the same commands will generate the same output, yet it is clearly a matter of art to input those commands. Whatever the output, every user can reformat, reorder, select, and consolidate at will, so each copy may be different.

And copies have copies unto the 3rd and 4th generations, and each is different.

Those questions raise all the issues of abridgments and abstracts under present copyright law -- which are very complex questions -- and then a great deal more. "A genuine and just abridgment" is entitled to copyright protection under English law. Use of abstracts relies upon the application of the "fair use" principle - the right to quote copyrighted works for purposes of scholarship, journalism, science, etc. There is a huge volume of literature on this. The normal rule is that copyright flows from the pen or typewriter of the author. The problem arises when someone takes a copyrighted work and from it draws up an abstract. This raises "fair use" questions. But what if the abstract is compiled and written by a computer. Depending on the length and similarity of the abstract to the original, it may be regarded as fair use, or it may be a violation -- but in a computer produced abstract who committed the violation. It could be argued that the recording of the written copyrighted material into computer code for abstracting is a violation of the author's exclusive right to translate. (1) The American law, however, makes the mere entry of program material into the computer for use by someone who is a rightful possessor of the material not a violation.

---

(1) 17 U.S.C., sec. 1(b). There is a broad view of "translation" which has deemed that written explanations of physics passed in mathematical representation are translations. (Addison Wesley Publishing Co. v Brown, 223 F. Supp. 219 (E.D.N.Y. 1963).

There is the fundamental question as to what computer uses are "reproduction" and which are "reading". In print that was a clear and simple distinction. No liability stemmed from reading a printed work, whether once or many times. Liability stemmed only from copying the work. In computer handling of text, however, that distinction (which was crucial for the concept of copyright) disappears. Every reading of computer output requires the regeneration of it; every reading is a printing. To attempt to apply the laws governing printing of texts to an activity which is functionally the reading of them, can only lead to total constipation in the intellectual process.

What sort of display of the material in the computer memory is publishing? Of course, if the text is a program it need never be displayed at all. The display may only be of its product. Who then is the author of the product which is published?

The idea that a machine is capable of intellectual labor is beyond the scope of any existing copyright statute. If the computer is not the author of something that is automatically produced then who is? And if the machine is the author, can a computer infringe someone else's copyright?

8.3 Potential Solutions

It has been suggested that difficulties can be reduced by imposing copyright liability at input instead of at output. (1)

(1) The UCC, definitely, and the Berne Convention, problematically, permit copyright liability to be introduced at point of input.

This solution would work with the computers of the 1970's, but will be vitiated by the systems of the 1980's.

In the past, a typical computer system that hosted a data base consisted of a stand-alone computer, or at most a few computers linked by dedicated wires in a self-contained network that conceptually constituted a single virtual computer. Code was entered by a typist or key-punch operator. The text was used by the same user group who had ordered it entered; it was stored in that groups' protected files, inaccessible to anyone else. If that data was to be made available to others by electronic publishing, first a contract had to be made; then the purchaser could get limited access to those files over a specialized network with which he also had a contract. In that sort of system, a royalty could be charged as a piece of copyrighted text was keyed into the computer. Even fair use could be reasonably well defined; the scholar entering data in his own computer files for his own use on his local machine could well be construed as a reader making fair use rather than as a publisher. The act of data entry was discrete and well-defined, and in the case of dispute, evidence could be established with a tolerable margin of error.

8.3.1 Future Computer Usage

Consider now the likely pattern of computer usage in the late 1980s. Most computers will be attached to the world's high speed

telecommunications network, and therefore linkable as if they were parts of one virtual computer. Intelligent terminals will be found on millions of desks and even in some homes, linked almost as informally as telephones are today via the same network to each other and to the computers. The owner of a file will be able to secure it against access by others, or if he wishes to publish the information, he will be able to open the material in his file to either specified others or to all others, as he wishes. The nodes on the network, however, will share a mailbox system whereby a person with access to one file will be able to send a copy of material from that file to anyone else's mailbox in any computer.

On such a system, a valuable text will not be entered from any one point, but will be created on the system by authors sitting at their terminals and typing rough draft into their electronic files. The text will be edited and revised at CRT terminals. There will be no moment of entry at which a valuable completed text comes onto the computer; it has been there all through conception, gestation, and birth. The point at which someone decides that it is a text for which he is willing to pay is not the point of entry.

8.3.2 Royalties:

To design an appropriate royalty system for such a pattern of text creation and distribution is not easy. We have already noted the difficulty of identifying the canonical version for

which payment should be made when the text is constantly changing. We have also noted the difficulty of keeping track of who sees what copy. Yet no workable system can levy a charge except at the point of use -- which is a basic flaw of the concept of liability at entry. The only time at which a charge can be effectively collected is when there is a user who wants the material and is willing to pay to get it out of the system.

When a 1980's author or publisher decides to make a text available for a fee, an obvious way to do it will be to put an access condition on his file, allowing others to read the material for a payment.

Four things should be noted about this arrangement, however. First, liability is incurred neither at input nor at output from the computer, but within the system. Secondly, what protects the author or publisher is physical control of the text for there is no count of its reproduction once it is out of his hands. Third, therefore, a billing system operated by the network is necessary if fee collection is to be easy; without that there is too much red tape in making arrangements for occasional access. Fourth, once the publisher's text has been read by anyone else, evasion of royalty payments is quite easy, because the reader can store the text in his computer and do whatever he wants with it; computer copying is even easier than xeroxing.

Today, most users of information bases read the output on rather slow dumb terminals, So they read only short information on line.

If they wish more output they order it off line, and typically get it in hard copy. In computer operations of the 1980's the reader will have the option of entering the data that comes to him at high speed into his own cassette, floppy disk, or bubble memory for local on-line perusal. He will thus have removed a potentially valuable text from the control of the publisher.

8.3.3 Problems with Computer Files:

Let us consider an example of typical 1980's usage of computer files:

Programmer Smith writes a proprietary program; archivist Schmidt creates a national accounts data base; user Hansen calls Schmidt's statistics and Smith's program to estimate the growth rate of employment in industry X; he reads the calculated growth rate figure on a CRT and copies it onto a piece of paper. In that simple situation a royalty charge could be levied at the point of accessing Smith's program and Schmidt's data.

However, if Hansen was planning extensive work with Schmidt's data and Smith's program, it would be more economical for him to copy them into his computer memory so as not to have to incur communications costs repeatedly. (As is well known, computing costs are falling faster than communications costs.) Smith can protect his program from such copying. He can set access so that others could use the program on Smith's own computer, but could not read it. That, however, requires that the data be sent to

Smith's computer and precludes Hansen from doing the analysis on his own computer where he may have specialized software or other facilities well adapted to his needs. Furthermore, the program would remain a black box that Hansen would have to trust and could not modify. So Smith's restrictive publishing service might be less attractive to customers than another one that took greater risks about its programs being copied. That is a marketing choice the program vendor has to make.

8.3.4 Data Base Vendors:

The vendor of a data base has less choice. His valuable possession is not a process, but the text itself. If he does not let it out he has nothing to offer. He may, indeed, follow a commercial strategy of marketing service more than text. He can try to update the data more promptly than competitors. He can offer unpublished programs for searching his archives. He may try various marketing strategies, but one of the least promising is prosecution of copiers in the courts. That was a good strategy for book publishers in the past, because a pirated edition was something produced in thousands of copies in a fixed location where the evidence and proprietorship could be established. It is not a good strategy against casual copying on photocopying machines or computers.

For governments a policy issue is how far to back publishers in their protective maneuvers. As always in public policy there are conflicting objectives. One objective is to provide means whereby

the creators of intellectual products can be reimbursed. Another objective is to allow free flowing diffusion of information and ideas. Another objective is to keep laws enforceable.

Clearly, laws can be passed extending protection to computer files, but can they be enforced? Deliberate penetration of locked computer files and copying them can be defined as theft. Contracts may prohibit rediffusion of data that is copied or that requires the return of the data uncopied after it has been read. But there are severe limits to how far such restrictions would be obeyed.

8.3.5 What International Agreements Are Workable?

Diversity among states in their intellectual property practices makes problems for each other; given the ease of transmission of data to more liberal jurisdictions, it is difficult for one state to enforce stringent rules. And so, for computer data, as for print in the past, there is reason to consider international agreements. What are some of the topics that such agreements might cover? We list what the Chinese might call "two yeses and two no's".

1. A convention or other agreement on principles could establish arrangements for collecting royalty fees from foreign customers. There are three components to the billing of a remote computer user; the communication charges, the computer charges for use of the remote host, and royalty fees for accessing particular files.

The bills can come from three different organizations: for example, the users's PTT, the owner of the remote host, and the owner of the files. Alternatively there might be one bill from the organization that manages the network and that acts as agent for the rest. There are clear advantages to a single bill. If each customer has to make prior credit arrangements with every file owner, the progress of on-line information systems will be much delayed.

The problem is particularly acute where the access is in one country and the purchaser in another. For the PTT to collect royalty charges for foreign data bases would be helpful, and be a source of revenue for PTTs.

2. A convention or other agreement on principles could facilitate the enforcement of contractual agreements between computer owners and file owners on the one hand, and their users abroad. Courts should give recognition to contracts entered into for using facilities located abroad.

3. It is probably impractical to suggest that second or third hand users, who use a copy of computer code without any contract should be subjected to any laws but the laws of the country in which they are physically located. If, as we suggested above, countries will differ for some time in the ways in which they adapt to the new situation of data communication, then countries that stringently require data users to respect restrictions laid down by data suppliers, can hardly expect countries that

experiment with more liberal policies to give the stringent laws extraterritorial sanction.

4. Similarly, a convention enacting uniform standards of liability for use of proprietary data or programs is premature. Property rights in data are a confusing and complex issue. It will be hard enough for individual countries to reach conclusions about policies through their domestic political processes. To do that through the labyrinth of international negotiations would be impossibly hard.

Whatever decisions are reached domestically or internationally will, as the dynamic technology of computer communication changes, turn out to be wrong in part. Correction of errors that are frozen into international agreements is doubly difficult. Thus wrong decisions in an international convention could seriously slow down development.

Hopefully, over the coming decades, common experience and sharing of views will lead to a certain convergence of practice in OECD countries regarding intellectual property. But that natural evolution would be hindered, not helped, by encasing experimentation in elaborate rules.

9. THE INTERESTS AT STAKE

Everything that we have said so far has suggested that

1. there are some prospective problems regarding transborder data flows, but few solutions by regulation;

2. application of established legal concepts such as copyright in the same way as they have been applied to print media is unlikely to work well and will make more problems than it will solve;

3. the technology is so dynamic that solutions based on the practices and systems of the '70s will be quite irrelevant within a decade.

That is not a counsel of despair. On the contrary, we would like to suggest that many of the problems that seem intractable when approached through legal concepts that grew out of old technologies will turn out to be very tractable when their users try to solve them in practice.

The point becomes clear if we look at the history of copyright not legalistically, but sociologically. In fact, copyright has never worked except when various vested interests in the process of intellectual production found it to their mutual interest to create a payments system, and when the payments system was based upon the specific features of the technology and market being used. No law, as such, has ever been able to create a property

right in information and successfully compel everyone to abide by it; information is too fluid an object to be thus controlled. What has been successfully controlled for payment purposes have been certain large scale institutions that engage in information business on a regularized and routine basis.

So, in this section we look at the emerging interests and institutions in the computer data field, to attempt to identify what the different major interests are, what convergences there may be in their interest in providing a payment system, and where the points of leverage may be that will permit effective collection.

We can do so in but a sketchy and preliminary way, for the technology is in its infancy and the institutions of computer communication are only now emerging. It will be at least a decade or two before the various interests and institutions begin to understand their needs, problems, and options fully, and begin then to establish the necessary practices to provide effective payment for information services. That will have to be done largely experimentally by the industry itself. OECD can play a useful role as a catalyst in these discussions, and as a forum in which the public interest can also be heard.

9.1 Authors and Licensors of Programming Material:

Software is rapidly becoming the largest part of the cost of new computer systems Yet it is hard to prevent pirating of software. In the computer hobby field there are constant laments about the

difficulty of getting amateur computer owners to pay reasonable prices for simple programs. Much unpaid copying onto magnetic tape cassettes and even onto records takes place. That mode of transferring programs is fairly common in the professional computer field, too. For programmers, little skill is necessary to copy a proprietary program and trade it to a friend in another installation. It saves time of filling out requistion forms, and, perhaps, the software will even come debugged, to boot!

Why, then does anyone invest in the multi-billion dollar software industry, one of the fastest growing in the US, and one of the easiestto enter in terms of capital outlay ? It is supported more for the services it gives than for the programs themselves. A program is no more than a series of instructions -- they may work or they may not, more often the latter. The software house sells interpretative skills, called program maintenance; they periodically update the program, help move it from one computer to another, or adapt it to an existing computer which may undergo continual modification of its control or operating system, or have additional hardware added. Computers are not static devices, and software must grow with each installation. Some concepts can be patented, (1) but as in most such protections of design inventions, the backup and technics needed

(1) In June 1978 the US Supreme Court (in Parker v. Flook) for the third time rejected a patent on a computer program. However, the Court held the door slightly ajar to the possibility that some programs could be patentable as "inventive applications" rather than mere verbal expressions or uses of principles of nature.

to make it work are often more important than the original discovery. Pirating of ideas goes on all of the time. It is deplorable, but has not totally disrupted either the economics of invention, nor has there been any evidence that clever minds will stop inventing because of lack of foolproof protection. It is doubtful that computers have done anything to change that situation save to make it even harder to be a mere copycat.

9.2 ASCAP-type Payments?

In a number of countries, royalty pools have been established to share income in situations where individual accounting has been impractical. In the United States for music, two such cartels (BMI and ASCAP) were formed to distribute revenues to their members.

Historically, after some initial controversy, mechanisms for dividing income streams were developed for broadcasting, records, and films, as they became a recognized element in the entertainment establishment. The music users in broadcasting and films, too, had large vested interests to protect, in continuing the supply of music and performers. Had they prevailed in early attempts to use material without sufficient compensation, the broadcast stations and film producers would have found their artistic sources all but dried up. Only the details of exactly what format or plot version was copyrightable remained for the courts, with litigation continually occurring in such minor matters. Wholesale theft of creative works would be unthinkable

today among the major elements of the industry, though pirating on the periphery accounts for about ten percent of the sales of the industry. Eventually, we expect, cable operators and videotape distributors will see it in their interest to support creative talent. The CATV industry already willingly accepted having to pay into a royalty pool under the new copyright law.

The question remains, can ASCAP-BMI-type of mechanisms be useful for collecting royalties on data transmissions, assuming the creative work can even be identified as such? It depends on who is issuing the work, and what the economic benefits are. Already similar, albeit informal mechanims have been set up to protect, or rather recompense publishers for the value-added functions of preparing and diseminating technical materials. The major industrial libraries in the U. S. have voluntarily agreed to "observe" the new copyright law (which they could have easily ignored) by paying "royalties" on each copy of a technical article made, with charges passed on, via internal accounts, to the user. These major corporate libraries will restrict copying to one iteration, or "fair use." If multiple copies are needed, the user will be asked to requisition printed copies from the publisher, unless unavailable or some urgency is indicated. But the libraries, of course, have their own self-interest in mind; the cost of these payments are minor in their operations, and the value of the publishers' services (many of them being technical societies) to the corporate research effort is perceived as large. Many of these societies, and private publishers, as well,

are supported by corporate contributions and government subsidy of one kind or another to keep them afloat. Royalties will be but another contribution. It should serve as an example of a possible outcome in the database society of the future, if a valuable function is being performed which must be shared by multiple users, that user community will find a solution, or be without. Where willingness of the users to cooperate in a system of compensation exists, computers have the advantage of containing within themselves the mechanisms for accounting, without imposing chores on the users.

9.3 Databanks:

Information in a pure form is one of the newest private industries. For decades it has been considered the province of governments, or quasi-governments to collect the data necessary for a modern economic system to survive: censuses, crop estimates, weather forecasts, etc. Some data sources have been contributed by stock exchanges or special interest groups, but, as with governments, most of the cost of collection and dissemination is not levied on the user. Data has been compiled, therefore, mainly when it has been in the compiler's interest to make its information available.

In the computerized information-oriented society of the present and near future, information may be finally recognized for its true value as a saleable commodity. The user community will cooperate to see that the databanks value-added services are

protected from erosion. Data with a short, but valuable lifetime, perhaps specifically processed for a customer, will be most saleable via data communications links. The economics of the marketplace will have to be worked out as it evolves; it is almost impossible to anticipate all the probable variations and provide legislation in advance since we have only vague ideas of the uses and sources, much less the medium of transmission, of future information.

Computers manipulate data in two ways:

1) as information to be processed 2) as information or instructions on how to process the data, loosely referred to as a "computer program".

With the earliest complex data network, the SAGE air defense system of 1955 which led to IBM's first large commercial computer, the 7090, the value of distributed processing for local data needs and network file transfer for global requirements was immediately obvious. Later versions of the 7090 were connected in tandem for real-time data protection such as the SABRE airlines reservation system in 1958. Tandem or multiple computers would access the same banks of storage devices, usually in the same room, to share data and programming instructions. More recently, improvement in communications and processing has permitted computers to access both data and instructions from remote sites. These distributed processing systems may swap programming information over long distances, turning networks of

machines into a virtual machine.

The emergence of a computer network into a virtual computer, highlights the two computer functions: Not only will networks transmit it relatively coherent data, but they will process the information as they transmit. The high-level synchronous line protocols do this in part by providing for error-correction, which is essential to the operation of any computer network; by addressing and routing data packets in a most efficient manner; and by aiding in translating code between differing machine types and subtypes. Some of the data being transmitted may be merely machine code, program subsets and micro-programs, as today large main frames swap programming parts between external files and main memory to create so-called "virtual machines". The virtual machine has the capability of expanding beyond national boundaries, and the bits it swaps back and forth between files and other CPUs may be only for machine efficiency's sake and have no meaning in terms of data transmission otherwise. Such traffic, even if monitored, would be uninterpretable.

Added to this complexity will be cryptographic techniques enabling bitstreams to appear meaningless, as if the machine code and the programmers language and dialect would not make the bitstream fairly meaningless to an outsider in the first instance, anyhow.

It is too early to tell where these concepts will go, but certainly the availability of wideband, high speed networks may

influence the design of computer systems in a fashion undreamed of only a few years ago. It would be unfortunate if the technological opportunity were restricted for reasons related to political boundaries. Furthermore, if such communications restrictions are enforced, the possibility that data processing would move to regions where highspeed computer networks were permitted, would be to the restricting nation's loss. Analogies can be made to other past restrictions on technological innovation which prevented growth of a valuable industry: delay in the introduction of railroads in certain European nations during the 19th Century to protect canal and highway interests; and restrictive labor practices which caused massive shifts in industrial employment.

What then of placing restrictions on databanks? And for what reason? Only total control of a datalink would be effective in controlling foreign access, and most likely such control would reduce usage. The flexibility of having ones' program or computer interact with another computer data source would have to be eliminated for control's sake. Reduced usage would serve neither the user nor the supplier of data. Control of the datalink would not serve even as protection for the copyright owner, since he would be worse off then before.

The most categorical case for data restriction is when there is a deliberate policy to prevent data of some kind from entering or leaving national borders. Such might be the case with personnel

information or military secrets. But with the nature of data networks as they are evolving, the best protection of such data is secure encryption, coupled with physical security at the data source. That kind of control, while it would permit any data external to a country to enter, would prevent its exiting.

Such protection of military or other sensitive information requires its control at the place of its storage. There is no plausible means to place controls over the content of information crossing a border, unless a country chooses to totally forgo the benefits of computerized database networking.

10. A PAYMENTS SYSTEM

Above we noted that transborder data flows are not economically viable unless there is international co-operation in a system of collection of charges. Some sorts of international data flows are much more affected by this problem than others. In the absence of any system other than what already exists among the carriers, there still would be a considerable volume of intracompany transactions within large multi-nationals, since in them the use of data, if any, are a purely internal transaction. On the other hand the absence of a system of charges for the data itself is likely to greatly inhibit the development of electronic publishing. So in what follows we consider the special but important case of creating a payments system for public data base services.

The costs of furnishing on-line information services may be divided into three categories:

that of creating the information and converting it into machine readable form;

that of maintaining it on random access memory with a suitable communications interface to to the network;

and the cost of searching for and transmitting to the customer a desired information service.

Creating and storing the information accounts for almost all the costs of operating the service, the incremental cost of selling an additional access to it are negligible. Under these circumstances non-payment by customers represents no out of pocket loss to the vendor and deficencies in the payments system are more tolerable than in the sale of goods.

Frankston (1) has pointed out the need for the financial system to be the servant of the participants. The right of the user to withhold payment for unsatisfactory service and vendors to deny further access to their service must be guaranteed. Disputes will arise and mechanisms for their resolution must exist.

One of the characteristics of services delivered by telecommunication is that the vendor and the customer need have no close contact with each other. They need not meet to bargain and press the flesh. Where the customer is a substantial institution, like a business, that makes little difference. There are established credit and collection mechanisms; the customer will not disappear; he has a large investment at hostage. In the case of small unit sales to consumers in their homes or in transit, the problem is quite different. Either the vendor must establish a large sales and collection organization, or he must somehow automate collection.

(1) Frankston J., The Computer Utility as a Marketplace for Computer Services, Project MAC Report MAC-TR-128, MIT, May 1974, p. 24.

There are various ways to automate collection. One is to have coin machines, like the copying machines in a library. That, however, requires special equipment widely distributed and therefore a large operation. Furthermore, it misses the opportunity for low cost dissemination created by the presence of TV sets and telephones as terminals. Thus one obvious solution is to turn either the phone company or the cablecaster into the bill collector. The one has established, the other hopes to establish, a widespread system of equipment which reaches every potential customer of the information services, which is also linked to the delivery of the services and has a billing and collection organization. The organization that provides the conduit could, for a fee, append to its bill charges on behalf of the service that was delivered over the conduit.

Thus one initially attractive model for the financial transaction system is the telephone network where the user deals with only one vendor, his local phone company, although service may be provided by many vendors (independent phone companies, foreign PTTs). All information vendors on the network would charge the network for services supplied, the network would charge each user for services received. Just as in the world telephone system, the PTT would do all the collecting within their own countries, and then only clear aggregate balances between countries.

An example of the PTT acting as the collector is the British plan for Prestel Viewdata (formerly called). Data suppliers deposit

their pages in the GPO's computer at a fixed charge (circa £ 1 per year.) The GPO exercises no selection or quality control. Subscribers dial up any page they wish onto their TV screen. For that they pay a connection charge, and, in addition, perhaps a fee to the supplier of the material read, depending on what the material is. Ads, for example, would normally be supplied free, the advertiser absorbing the deposit fee. Other publishers will charge for the information displayed (the subscriber being informed at the time that he dials in). All charges appear on the subscribers monthly bill.

There are problems, however. Unlike telephone service where the number of suppliers is limited, the product standardized and little subject to quality variations, the information market will be characterized by many vendors selling different products of varying quality at a wide range of prices. No one bad phone bill is very large. A computer bill may be. Also the foreign settlement in the telephone case is with another phone company. In the information services case it is with many vendors. Some customers might run up astronomically high bills, and sometimes inadvertently. While the telephone model is applicable for the sale of data communications services between different networks, the inclusion of computing and information publishing costs in the communications billing system seems unlikely to seem attractive to many telephone companies.

Another model is that of the air and rail transport system where payment for the product is separated from payment for transportation but where that carrier which serves the point of origin, bills the customer on behalf of all carriers involved in the shipment to destination. This model envisions an information vendor, upon receiving a request for service which would include the requestor's credit reference, verifying that credit with the referenced institution over the network before the provision of service.

10.1 A Less Optimistic Projection:

Another plausible model is one in which on-line information services to small consumers comes widely only with the arrival of electronic funds transfer systems for the same population. EFT also requires a widespread system with fairly universal acceptance and adequate controls over the behavior of its users. Once that system has reached the individual household (and that will not be soon) then there will be a bill collecting mechanism reaching virtually every customer electronically. It is at least possible that mass information utilities, as distinct from professional and business ones, will have difficulty diffusing widely before that time.

Involved is the question of authenticating the identity of the credit requestor. With a sufficiently low communication cost, the requestors voice could be digitally encoded and transmitted

to the credit verifying institution for comparison against a reference voiceprint. Alternative scenarios utilizing passwords exchanged between user and credit institutions may be imagined. Whether the economics of information services will require such a degree of security will most likely emerge only with experience.

These problems of creating a viable system for billing small buyers of services for many casual sales by numerous small vendors, when there is no contact between them, seem difficult enough domestically. They are even worse internationally. One can imagine that many vendors will not choose to respond to retrieval requests or other such enquiries that come from remote countries where they have no established financial arrangements. This may become a strong argument for organizations like PTTs acting as middlemen in the process.

All of these considerations may perhaps alternatively push many vendors of international information services to one of two other arrangements: wholesaling through a local intermediary, or subscription arrangements in advance, perhaps for unmetered or liberally metered service. The communications technology does not require local intermediaries. Low cost direct access across the globe, is, as we have seen, increasingly possible. but fiscal considerations may impel vendors to route their information through a locally franchised agent. The alternative of advance subscriptions to relatively unlimited services also corresponds to the economics of the industry, for the variable costs of extra

enquiries to the data base is small. Perhaps the door-to-door magazine salesmen of the year 2000 will be selling data base services.

How the international use of data services will grow we cannot now know, though we can be very confident that it will happen. These various alternative organizational schemes for payment need to be studied, and perhaps legal and financial arrangements worked out. International organizations such as OECD can play a very useful role in facilitating the creation of organized systems of international payment for public data base services.