

DOCUMENT RESUME

ED 367 351

IR 054 899

AUTHOR Borod, Elizabeth A.
 TITLE An Annotated Reference Guide on International Telecommunications and Transborder Data Flow for Library and Information Science Professionals.
 PUB DATE Nov 90
 NOTE 81p.; M.L.S. Research Paper, Kent State University.
 PUB TYPE Dissertations/Theses - Masters Theses (042) -- Reference Materials - Bibliographies (131)

EDRS PRICE MF01/PC04 Plus Postage.
 DESCRIPTORS Annotated Bibliographies; Communications; Computers; Information Dissemination; Information Management; Information Networks; Information Science; Information Sources; Information Technology; *Information Transfer; *International Communication; Laws; Legislation; Library Research; Library Science; Standards; *Telecommunications

IDENTIFIERS *Transborder Information Flow

ABSTRACT

The purpose of this guide is to provide library and information professionals with a brief history of telecommunications and transborder data flow (TDF) as well as an annotated listing of available resources and organizations concerned with these topics. The bibliography is organized into 14 themes: (1) communication--international; (2) computer--international cooperation and standards; (3) computers--political aspects; (4) information networks--standards; (5) information services--international; (6) information technology; (7) library science--technological innovations; (8) research organizations; (9) telecommunications--bibliography; (10) telecommunications--law and legislation; (11) telecommunications--library and information science; (12) telecommunications policy; (13) telecommunication standards; and (14) transborder data flow. The guide emphasizes the importance of remaining aware of newly created standards, treaties, laws and conventions as well as restrictions on use and availability of information. Two additional resources are appended: "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" and "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." (TMK)

 * Reproductions supplied by EDRS are the best that can be made *
 * from the original document. *

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION
CENTER (ERIC)

- This document has been reproduced as received from the person or organization originating it
- Minor changes have been made to improve reproduction quality
- Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

ED 367 351

AN ANNOTATED REFERENCE GUIDE ON
INTERNATIONAL TELECOMMUNICATIONS
AND
TRANSBORDER DATA FLOW
FOR LIBRARY AND INFORMATION SCIENCE
PROFESSIONALS

A Master's Research Paper submitted to the
Kent State University School of Library Science
in partial fulfillment of the requirements
for the degree Master of Library Science

by

Elizabeth A. Borod

November, 1990

"PERMISSION TO REPRODUCE THIS
MATERIAL HAS BEEN GRANTED BY

Rosemary Du Mont

TO THE EDUCATIONAL RESOURCES
INFORMATION CENTER (ERIC)."

BEST COPY AVAILABLE

12054899

ABSTRACT

The increased globalization of information services, telecommunications and transborder data flow (TDF) of information has many consequences for library and information professionals. Much of the present literature addresses primarily business and legal aspects of telecommunications and TDF, although there is an increasing focus on the implications for libraries. The purpose of this guide is to provide library and information professionals with a brief history of telecommunications and TDF as well as an annotated listing of available resources and organizations concerned with these topics. With constantly changing technology and resources, information professionals must remain aware of newly created standards, treaties, laws and conventions as well as restrictions on use and availability of information.

Master's Research Paper by
Elizabeth A. Borod
B.A., Cleveland State University, 1988
M.L.S., Kent State University, 1990

Approved by

Adviser Thomas J. Froehlich Date 12/10/90

LIST OF ACRONYMS

| | |
|-----------|---|
| CoE | Council of Europe |
| ECMA | European Computer Manufacturer's Association |
| EEC | European Economic Community |
| IT | Information Technology |
| ISDNs | Integrated Services Digital Networks |
| IIC | International Institute of Communications |
| ISO | International Standards Organization |
| INTELSTAT | International Telecommunications Satellite Organization |
| LSP | Linked Systems Project |
| NISO | National Information Standards Organization |
| OSI | Open Systems Interconnection |
| OECD | Organization for Economic Cooperation and Development |
| TDF | Transborder Data Flow |
| UPU | Universal Postal Union |
| WIPO | World Intellectual Property Organization |

INTRODUCTION

Transborder data flow (TDF), originally addressed in 1974, may be defined as the exchange of information across national borders via telecommunications. The implications of TDF affect many areas of information collection, arrangement and dissemination, and thereby have increasing significance for the library and information service professions. When looking at any aspect of TDF, one must also be aware of the role that international telecommunications plays in this transfer of information. The two are inextricably connected.

The issue of TDF was originally addressed by international organizations including the Organization for Economic Cooperation and Development (OECD) and the United Nations Educational, Scientific and Cultural Organization (UNESCO). Their involvement resulted in various guidelines and subsequent national laws and conventions governing the protection of privacy and transborderflow of data. Yet a lack of solid transborder controls exists, especially with the spread of open networks, perpetuating a variety of problems.

Most published materials addressing TDF focus on issues of personal privacy, national sovereignty and economic concerns. Much of this literature appears in business and legal periodicals. There is an increasing tendency to address this issue in library and information science literature, especially in regards to access rights, liability, the use to which the data is put, and the implementation of standardized information technology and equitable international policies which will facilitate and regulate the

international flow of information. The most important of the technology issues is the adoption and implementation of the Open Systems Interconnection (OSI) Seven-Layer Model.

Several issues, besides those already listed, affect the librarian and information professional, especially in situations regarding access decisions. Critical and professional judgement is required in order to avoid jeopardizing the national economy in which these professionals work, and the policies of their organizations. Current awareness of guidelines, including those of the National Commission on Libraries and Information Science (NCLIS), and the International Federation of Library Associations (IFLA), is essential in today's information field.

This reference guide is aimed at providing information professionals with an annotated listing of available sources such as monographs, periodicals, articles, conference proceedings and international government documents, and the research and government organizations and "think tanks" which address TDF and international telecommunications policy, in order to best represent the needs of their clients, while avoiding conflict with their employers and their country's information policies.

A vital aspect of researching TDF and international telecommunications is defining the appropriate subject headings to search. The literature search should encompass more than academic- and library-related indexes. Searches should also be conducted in legal and business sources in order to obtain the most comprehensive listing possible. Additional searching may be

TDF was first introduced, as a concept, in 1974 at a seminar sponsored by the OECD, where the focus was on personal privacy. In 1977, at a symposium also sponsored by the OECD, the discussion focused on the fact that non-personal and business data were no longer safe. This led to the consideration and implementation of legislative restrictions to safeguard information. Further concerns revolve around the impact of TDF on trade, productivity, competitiveness, employment and national sovereignty.

In 1978, an OECD expert group on Transborder Data Barriers and the Protection of Privacy, was established. Their goal, to develop guidelines for basic rules governing the flow of personal data and the protection of privacy, and to investigate the legal and economic problems related to the flow of non-personal data, led to the establishment of the 1980 "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." (These guidelines are included in this guide, as Appendix One, in order to provide the researcher with a valuable historical document). The intent here was to ensure data protection in both private and government sectors.

Another organization involved in early TDF issues is the Council of Europe (CoE). A long-time proponent of data protection activities, the CoE's true orientation is represented in the 1981 treaty, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." (This document is included, as Appendix Two, for comparison as well as for its historical value). The activities of the CoE have been aimed at

creating a consistent approach to TDF within and outside Europe.

The literature on TDF is, indeed, varied and far reaching. Certainly, many issues and concerns overlap. At present, with international boundaries breaking down, there is a move away from the theoretical issues of regulation, sovereignty, and information integrity/security, towards the technical aspects of information transfer and to accept the inevitability and dependency on it. Also, there are concerns about information imperialism where information superpowers such as the United States, Canada and Western Europe, control and manipulate the actual information as well as the means to access and acquiring such data. Many lesser-developed nations are becoming involved in this arena which more frequently is being discussed in TDF and international telecommunications literature. The issues of loss of control of information, dependency on technology and/or information, and cultural impact constitute a major portion of the current controversy on TDF.¹

As for libraries' involvement with TDF, the IFLA International Program for Universal Dataflow and Telecommunications (UDT), hosted by the National Library of Canada, publishes a newsletter as well as sponsors research and activities related to TDF.

The IFLA Transborder Data Flow Survey of 1986 provided significant new information in relation to barriers to TDF involving libraries. The three principal barriers were found to be

¹ Bender, David R., "Transborder Data Flow: an Historical Review and Considerations for the Future," Special Libraries 79 (Summer 1988): 233.

of information technology nor have developed sufficient tools for evaluating the technologies to make crucial decisions.

There exists a very strong need to interconnect library systems, which is where the Open System Interconnection (OSI) Seven-Layer Reference Model is often cited as the most appropriate example. An example of a library network based on the OSI model is the Linked Systems Project (LSP) which allows the Library of Congress, the Research Library Group, the Western Library Network, and OCLC to share and exchange data among their various kinds of computer systems.

The convergence of telecommunications and technology is resulting in greater decentralization of information processing capacity. The possibility now exists of integrating voice, video, and data communications networks. Telecommunications networks are providing higher speeds and increased bandwidth capacity through the conversion of analog to digital transmission.⁴ The above described advances in combination with TDFs will lead to greater resource-sharing in a world whose borders are quickly disappearing.

Much of the available information on protocols, linked systems, and the OSI reference model is purely descriptive. It is often a chore to obtain a document which provides a clear overview and perspective on the overall relation of protocols or standards activities to computer networking. It is, therefore, advisable to review a variety of materials in order to obtain a comprehensive

⁴ Bigelow, Linda and Alice Calabrese, "Libraries and Telecommunications Technologies," College and Research Library News 50 (March 1988): 198.

costs, training and awareness.² It was interesting that respondents to the survey placed little emphasis on the policy and legal factors which have figured prominently in the general TDF literature. The flows in question would be on-line or off-line and included electronic messaging. As analyzed by library application, the following are the most important aspects of TDF: citation retrieval, cataloging, inter-library loan, and acquisitions.

The most prominent barriers to TDF involving libraries are as follows.

Cost was cited as a barrier much more frequently than any other by national libraries and national library associations. Database service providers...related cost as the second most important barrier: for them; training, education and awareness was the most significant barrier. In descending order of frequency, cost barriers mentioned in responses were: costs of establishing, maintaining and using databases; telecommunications costs; staff and staff training costs; software costs. Technical barriers in the same order were: incompatibilities in services, systems, hardware and software; physical/technical limitations; computer/communications standards; reliability of communications.³

A review of this survey is vital to any information professional and is available, free-of-charge, from the IFLA International UDT Core Program office.

Integration of telecommunications into library services is a hot topic of the 1990s. Identification of telecommunications technologies and adaptability to the needs of libraries is frequently cited in the literature. The problem is that librarians have often been unable to keep up with the rapidly changing field

² Duchesne, Roddy, "IFLA Transborder Data Flow Survey," UDT Newsletter 2 (August 1987): 1.

³ Ibid, 3.

view of the topic. One aspect to acquaint oneself with is with protocols which are a set of rules by which two computers or other electronic devices can exchange data for some purpose. This covers agreements on dialog and format of the data being exchanged through services, often constructed through the use of a layered set of protocols.

Another aspect of resource sharing is to develop a standard, an agreement reached by a group of people or organizations to do something in a common way. This is a vital aspect of TDF in that strict universal adherence to standards will ensure the smooth flow of information. One organization, the International Standards Organization (ISO), an international standards body made up of national standards groups from many countries, is especially important due to its popularization of the term "reference model," and especially for its hand in developing the Seven-Layer Reference Model for OSI.

In any study of protocols and standards development, one should pay close attention to the various national networking environments. Furthermore, there exists the problem of incompatible major standards being used alongside one another. Problems of performance, complexity and the cost of conversion, and variables of organizational taste, functionality and the presence or absence of vendor support continue to plague many networking environments.⁵

⁵ Lynch, Clifford, "Protocols in Perspective," ASIS Bulletin 11 (August/September 1985): 11.

It is important for the library and information professional involved in international telecommunications and TDF to approach the literature in its broadest sense.

Much of the current library and information systems literature focuses on the application of networking; yet it is equally important for the practicing professional to have a current working knowledge of the telecommunications infrastructure upon which these applications are built. This is particularly true since the telecommunications infrastructure is extremely dynamic, and the effectiveness of many network applications will be determined by the form this infrastructure takes in the future. To be optimum, future applications must be targeted toward the environment in which they will exist and operate. At a minimum, they must be able to compensate for change in the environment, especially because of the magnitude of investment required by their endeavors.⁶

This brief introduction is intended to provide researchers with a general background of the issues related to international telecommunications and TDF. Because of so many related subject areas, one often has to broaden their search before they can narrow their search topic in order to obtain the most relevant materials. It is very advisable to acquaint oneself with the organizations involved in researching specific areas. Their journals, bulletins and newsletters are very useful and are often available free-of-charge.

It would be impossible to list here all the journals and periodicals that cover these issues and, due to rapid change in the technology, it would be futile because of the constant generation of new material. One should acquaint themselves with a variety of sources and then decide which are most applicable to their

⁶ Learn, Larry L., "Networks: the Telecommunications Infrastructure and Impacts of Change," Library Hi-Tech 6 (1988): 13-14.

situation.

We may expect a continuation of the increase in volume and import of point-to-point transfers of digital electronic data across national boundaries. While TDF will increase, that of information services and libraries will probably remain a small percentage of total world TDF. This is especially due to the volume of expansion in the TDF of other sectors. In fact, there is a move away from the concept of TDF, by the OECD Working Group on Transborder Data Flows, towards the idea of international data services, the point here being that TDF issues should be considered within the context of international data services.

As for the internationalization of telecommunications, there is likely to be an increasing level of international activity and debate working in the direction of harmonizing national laws, regulations and approaches where it becomes apparent that this is in the common interest. Ideally, this activity will result in the creation of an effective, international regulatory framework.⁷

TDF and international communications are an exciting aspect of today's global information society. As international boundaries break down, especially in the European Community, Pacific Rim, United States, Mexico and Canada, the need to technically and politically facilitate the exchange of data is especially vital. By surveying the historical, theoretical and analytical literature, one will obtain the most comprehensive view of these issues.

⁷ Kent, Allen, ed. Encyclopedia of Library and Information Science Vol. 45, Supp. 10, (New York: Marcel Dekker, Inc., 1990), s.v. "Transborder Data Flow," by Roddy Duchesne and Anna Levin.

REFERENCES

- Bender, David R. "Transborder Data Flow: An Historical Review and Considerations for the Future." Special Libraries 79 (Summer 1988): 231-235.
- Bigelow, Linda and Alice Calabrese. "Libraries and Telecommunications Technologies." College and Research Library News 50 (March 1989): 195-199.
- Duchesne, Roddy. "IFLA Transborder Data Flow Survey." UDT Newsletter 2 (August 1987): 1-12.
- Kent, Allen, ed. Encyclopedia of Library and Information Science Vol. 45, Supp. 10. New York: Marcel Dekker, Inc., 1990. S.v. "Transborder Data Flow," by Roddy Duchesne and Anna Levin.
- Learn, Larry L. "Networks: the Telecommunications Infrastructure and Impacts of Change." Library Hi-Tech 6 (1988): 13-27.
- Lynch, Clifford A. "Protocols in Perspective." ASIS Bulletin 11 (August/September 1985): 9-11.

COMMUNICATION--INTERNATIONAL

Cooper, James Arlin. Computer and Communications Security: Strategies for the 1990's. New York: McGraw-Hill Book Company, 1989.

The objectives of this book are three-fold. The first is to provide an information resource on the status of computer security techniques that will be available in the 1990s. The second is to provide an analytical basis for making quantitative assessments, especially valuable for its currency. The third is to survey the threats of which security practitioners should be aware. This book, useful for graduate-level courses, provides an overview of the study of computer and communications security, and a review of six particular aspects of the study: physical protection, personnel considerations, legal and regulatory aspects, hardware security, software security and network security. The final chapter addresses a global approach to security and discusses future issues. It includes an extensive glossary.

In the regulatory security environment section, relating to TDF, there is an international topics section which outlines international forums and the regulatory environments of the following countries: Great Britain, Canada, France and Sweden.

Dougan, Diana Lady. Communications Satellites: Challenges of the Future. Washington, D.C.: U.S. Department of State, Bureau of Public Affairs, Office of Public Communication, Editorial Division, 1988.

This is an address by Ambassador Diana Lady Dougan, U.S. Coordinator and Director, Bureau of International Communications and Information Policy, before the Great International Celebration of Satellites in Space sponsored by the Society of Satellite Professionals, Washington, D.C., October 16, 1987. Dougan focuses on the intrinsic merits of satellite and cable technology, and the potential ability of marketplace forces to lead an efficient distribution of traffic over both satellite and cable. She stresses the need for less government protection of one technology versus another. Further discussion focuses on striking a balance in the domestic and international regulatory framework that will let technology flourish, based on real markets and real requirements. The author encourages satellite professionals to commit themselves to the three concepts of innovation, adaptability and motivation in their research and practical applications of satellite technology. Good source for a brief 30-year history of the satellite industry.

Gonzalez-Manet, Enrique. The Hidden War of Information. Translated by Laurien Alexander. Norwood, New Jersey: Ablex Publishing Corp., 1988.

The author focuses on the varied socioeconomic changes brought about with new information technologies including how vast telecommunications systems have necessitated major reorganization of management controls/standards, and production and services. By focusing also on the political aspects, especially in regards to less-developed countries, the author explores several issues about international communication, with interesting coverage of the monopoly of information by the more technologically privileged. In a discussion of international information systems, the author focuses on how multinational corporations have contributed to the global expansion of information including the benefits and disadvantages of such message flows. It includes a vast bibliography with several Latin-American sources.

Mowlana, Hamid. Global Information and World Communication: New Frontiers in International Relations. New York: Longman, 1986.

This book provides an interesting overview of the global flow of information and world communications systems by examining both the human and technological dimensions. The author addresses the phenomenon of the international flow of information in the political, economic, cultural, technological, legal and professional contexts. Includes an extensive bibliography and index.

TDF is examined in chapter five, "The Political Economy of Information." A brief history of TDF is given as well as a description of actors and participants in TDF, the types of TDF, major issues and impact of TDF, and the direction of research. Includes notes. Like many other TDF specialists, the author points out how there are many changes in global communications yet to be expected as technologies continue to change traditional economic and political perceptions of information exchange.

COMPUTERS--INTERNATIONAL COOPERATION AND STANDARDS

Transnational Data and Communications Report. Washington, D.C.:
Transnational Data Reporting Service, Inc. Monthly.

This monthly publication addresses international cooperation between computers, and computer access control, data protection and electronic data processing. Each issue contains approximately six special interest articles in combination with the regular departmental features: Newsletter, International Outlook, Special Report, Freedom of Information, Data Protection, Documentation, Book Review/Source Data, and a calendar listing conventions and other gatherings of interest. Although focusing mainly on the business aspects of information exchange, this publication is very useful for all information professionals, and is one of the only periodicals, focusing specifically on TDF, that is published in the United States.

COMPUTERS--POLITICAL ASPECTS

Murphy, Brian M. The International Politics of New Information Technology. New York: St. Martin's Press, Inc., 1986.

This book focuses on the development and implications of the world information technology (IT) industry. The nine chapters discuss pertinent issues, including the concept of information colonialism, the foremost nations and agencies involved in IT, the actual transfer of information and the future of this industry.

TDF and international standards are covered in one chapter, including coverage of the following: the data dependence of multinational corporations and industry; national sovereignty; control of information flow; personal privacy; the CoE convention; OECD; the information technology of France, Canada, Brazil; INTELSTAT; WIPO; technical standards; OSI; ECMA; ISO; ISDNs, and the EEC. It includes a bibliography and index.

INFORMATION NETWORKS--STANDARDS

National Information Standards Organization (U.S.). American National Standard for Information Retrieval Service Definition and Protocol Specification for Library Applications. ANSI/NISO Z39.50 - 1988. New Brunswick, NJ: Transaction Publishers, 1989.

The specific OSI application layer service defined here allows an application on one computer to query the database of another. This information is essential in terms of understanding the procedures and structures of one search request, the request for the transmission of database records located by a search, responses to the requests, and access and resource control. Though not necessarily international in scope, the generality of this protocol will allow it to accommodate the addition of new services as required. It includes a list of the voting members of NISO.

INFORMATION SERVICES--INTERNATIONAL

Chartrand, Robert Lee. International Information Exchange: Relevant Activities of the White House Conference on Library and Information Services. Prepared for the Subcommittee on Education, Arts, and Humanities of the Committee on Labor and Human Resources, United States Senate. Washington, D.C.: U.S. Government Printing Office, 1980.

This study examines the role of library and information services in increasing international understanding and cooperation, as reflected in the White House Conference on Library and Information Services deliberations, resolutions, and documentation. This overview includes an executive summary and introductory section which outlines the significance of this area. The activities of the conference are then described, including: commentary by feature speakers, open hearing presentations, delegate discussion group action, and the final plenary resolutions and recommendations. A final section discusses possible ways of implementing the solutions via the public and private sectors. The document concludes with a series of appendices which contain background material.

This document is especially useful to the librarian and information specialist who seeks a historical perspective of international cooperation in information services.

INFORMATION TECHNOLOGY

Whitaker, Marian and Ian Miles. Bibliography of Information Technology: An Annotated Critical Bibliography of English Language Sources Since 1980. Hants, England: Edward Elgar Publishing Limited, 1989.

This bibliography includes over 500 annotated references on information technology including: the technology, social trends, the international economy, the employment debate, the quality of working life and work organization, industrial

structures, organizational issues, household and community, community and politics, and bibliographies and indexes. Each chapter includes an introduction to inclusive sub-chapters roughly indicating contents of each and reasons for the materials' inclusion.

LIBRARY SCIENCE--TECHNOLOGICAL INNOVATIONS

Adams, Roy. Communication and Delivery Systems for Librarians. Hants, England: Gower Publishing Company Limited, 1990.

Unlike other publications, this book begins with a glossary of telecommunications and computing terms indicating the relative import of jargon in this field. The remainder of the book deals with various communications and delivery systems including the development of communications technology, wide-area networks, local-area network technology, local- and wide- area networks in libraries, large-scale storage devices including library applications, artificial intelligence, recent communications technologies and social implications, including transborder data flow, possible scenarios, and libraries and the communications environment. Rather than solely a theoretical or technical perspective, the human perspective of information transfer is addressed in nearly every chapter indicating the inevitable association of people and technology. Each chapter includes an extensive list of references.

Crawford, Walt. Current Technologies in the Library: an Informal Overview. Boston: G.K. Hall & Co., 1988.

This valuable handbook discusses, in two parts, all publishing media circulated by libraries and all aspects of automation, including computers and communications systems. Through a discussion of each of these technologies, the author clearly defines the history, purpose and advantages of each.

Telecommunications are discussed as related to their enhancement of current library services and other possible applications. The telecommunications chapter discusses the fundamentals: information, transmitters and receivers, communications links, protocols and agreements; high-capacity communications links: coaxial cables, microwave communications, satellites, and fiber optics; equipment and long-distance telecommunications: modems, packet switching; telecommunications and libraries, a summary and a brief selected reading list. This source is especially helpful due to its easy-to-read-and-understand discourse and would serve as a good introductory text to anyone considering automation and publishing media.

Dewey, Patrick R. Fax for Libraries. Westport, CT: Meckler Corp., 1990.

In a discussion which intimates that fax technology is easier to operate than a personal computer set-up for fax transmissions, the following aspects of fax are discussed: technology, libraries, selection of a standalone machine and management issues, alternatives, and resources. Especially helpful is a directory of popular fax makes and models, and vendor addresses for PC fax boards and modems, and fax machines. By focusing on the issues of compatibility, transmission time, resolution, papers, standalone/PC/online/fax and cost, library use of fax is detailed with useful, timely examples.

RESEARCH ORGANIZATIONS

Atwater Institute. The World Information Economy Centre. 1625 de Maisonneuve West, Suite PH-211, Montreal, Quebec, Canada, H3H 2N4.

The Atwater Institute is an independent public policy forum, begun in 1985, which focuses on international issues raised by new computer and communication technologies. Recognizing that developments in computers and communications have merged, the Institute is concerned about the subsequent effects on individuals, industry and governments in relation to services, manufacturing and the virtual elimination of location as a factor in the competitiveness of nations. The Institute intends to promote informed policy-making at the international level. It conducts research, organizes international meetings and specializes in bringing together people with divergent interests and backgrounds for the constructive exchange of views. The Institute publishes a newsletter and also sponsors a variety of other publications.

Council of Europe (CoE). Palais de l'Europe, 67006 Strasbourg CEDEX, France.

The Council of Europe (CoE), consisting of twenty-one member countries, has a mandate to implement and enforce the European Convention on Human Rights of 1950. A long-time proponent of data protection activities, the CoE's true orientation is represented in the data protection treaty, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." The Convention provides rules of data protection, provisions concerning TDF, a system of assistance between signatory states and the establishment of a consultative committee to review its

operations. This convention is an attempt to control and regulate the handling and transfer of data within and outside Europe.

International Bureau for Informatics (IBI). Viale Civiltà del Lavoro, 33, P.O. Box 10253, 00144 Rome, Italy.

The scope of the IBI is to assist people, especially in developing countries, in the field of informatics, to help them live in the context created by this discipline, to better understand its impact on society and to derive the maximum benefits from its possibilities. It undertakes to promote the development and diffusion of informatics by advising, promoting and recommending the adoption of national and international policies for informatics, improved administration of informatics, and education in and about informatics. Part of the Bureau's work includes working on the uniform protection of TDF of the following countries: France, Iraq, Iran, Israel, Italy, Jordan, Lebanon and Spain. Through a series of conferences, publications and studies, the IBI has contributed to the increased awareness of the need to plan and guide developments in informatics and its applications.

International Institute of Communications (IIC). Tavistock House East, Tavistock Square, London, England, WC1H 9LG.

The IIC is an independent, international, non-governmental, non-profit organization concerned with international communications. In operation since the 1960s, with individual, institutional and corporate membership, the Institute provides an interdisciplinary forum for people in the field of communications including broadcasting, telecommunications, journalism, law, academia, industry and government. Dedicated to the analysis of all aspects of communications, the IIC obtains funding, and accepts commissions for independent inquiries and studies. The IIC works through seminars and meetings, aiming to bring together many disciplines, especially via its annual conference. The Institute also operates an extensive, specialized library of various communications media.

OECD. Handbook of Information Computer and Communications Activities of Major International Organizations. Paris: OECD, 1980.

This useful handbook was created by the Working Party on Information, Computer and Communications Policy (ICCP), at the OECD, which was formed in 1977, in recognition of the

increasing merger of information, computer and telecommunications technologies. It includes a listing of 48 organizations, governmental and non-governmental, including for each: organization name and abbreviation, addresses, main aims and objectives, origin of the organization and present number of member countries, organizational structures, activities in the field of information, computers and communications including conferences, seminars, publications, etc.

Organization for Economic Cooperation and Development (OECD). 2, rue Andre Pascal, 75775 Paris CEDEX 16, France.

The OECD was set up under a Convention signed in Paris on December 14, 1960. The OECD aims to promote high economic growth, employment and standards of living in member countries, to encourage economic development in both member and non-member countries and to contribute to unbiased world trade on a multilateral level in accordance with international standards. The 24 members include: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The OECD produces a variety of publications related to all aspects of international information transfer. These documents are especially useful for their currency and vast subject coverage.

Universal Dataflow and Telecommunications (UDT) Core Program of the International Federation of Library Associations and Institutions (IFLA). National Library of Canada, 395 Wellington Street, Ottawa, Ontario, Canada, K1A ON4.

The UDT Core Program's aim is to act as a support program to the activities of other core programs and IFLA Divisions and Sections concerned with electronic transfer of data. The primary focus of the program is on the technical, economic and policy aspects of electronic transfer yet it also aims to reduce barriers and to promote electronic transfer of data for the benefit of the library community and interrelated sectors.

The UDT Core Program is heavily involved in the technological issues involved in the development, implementation, use, maintenance and enhancement of standards for data interchange. By sponsoring seminars and publishing an irregular newsletter, UDT Newsletter (in English and French), the UDT Core Program is a valuable organization working directly with TDF-related issues.

TELECOMMUNICATIONS--BIBLIOGRAPHY

Snow, Marcellus S. and Meheroo Jussawalla. Telecommunication Economics and International Regulatory Policy: An Annotated Bibliography. Westport, CT: Greenwood Press, 1986.

This bibliography is a compilation of both authors' work with the main focus being on references dealing with both telecommunications and regulatory economics, especially those with an international focus. The book is divided into three parts covering the conceptual and theoretical background of telecommunication economics; the technological, institutional and legal framework; and empirical, policy and future studies; and research agendas. It includes both an author and subject index. TDF and other aspects of information transfer are covered in a variety of chapters.

TELECOMMUNICATIONS--LAW AND LEGISLATION

Branscomb, Anne W. Toward a Law of Global Communications Networks. The Science and Technology Section of the American Bar Association. New York: Longman Communications Books, 1986.

The various chapters of this book deal with international information networks in private and public sectors, multinational corporations, government agencies, and nonprofit institutions. The book aims to familiarize members of the Bar with changes in the international communications environment; the legal implications of technology on commercial transactions, diplomatic relations and transnational transport systems; and to assist in the development of telecommunications policy development.

The book focuses on three broad areas: the global communications environment; global information users and information transfer systems; and the emerging legal and policy issues in global information flow. It is an excellent source of easily understandable legal information useful to information professionals. It includes a bibliography and index.

OECD. An Exploration of Legal Issues in Information and Communication Technologies. Paris: Organization for Economic Co-Operation and Development, 1983.

This book contains two reports prepared for the Committee for Information, Computer and Communications Policy. The main focus is on whether the development of computer and

communications technology is outpacing the existing legal and regulatory framework. The first article deals, in general, with the legal aspects of the application of information technology. In doing so, it addresses privacy protection; freedom of information; vulnerability, unemployment and crime; conflicts, sovereignty, and protectionism; intellectual property, business law, liability, and insurance; evidence law and legal profession; institutional responses and profits. The second article concentrates on the legal problems related to transborder data flows by defining basic terms and concepts, the elements in existing international law and concludes with assessments and implications.

Pipe, Russell. A Business Guide to Privacy and Data Protection Legislation. Paris: ICC Publishing S.A., 1981.

Though directed at the business community, this guide is useful for those in need of the privacy legislation in seven countries including Austria, Denmark, France, West Germany, Luxembourg, Norway and Sweden. Basically, the laws cover personal data held by public or private sector organizations but also address a variety of other data-related issues. The guide also includes descriptions and full text of international agreements on data protection of the OECD and Council of Europe. This is a useful tool regarding country-specific background information and TDF legislation.

Ploman, Edward W. International Law Governing Communications and Information: a Collection of Basic Documents. Westport, CT: Greenwood Press, 1982.

Divided into ten parts, this book covers all aspects of international communications and information. It addresses the history, structure, standards and international organizations concerned with general international law; information, telecommunications, postal informatics and space law; intellectual property rights; trade and customs regulation; culture and education; and national security and law enforcement. It is an especially useful source for it provides a comprehensive assembly of nearly all major international legal instruments which affect communications and information, which are easily located in the alphabetically arranged list of instruments. It includes an index.

TELECOMMUNICATIONS--LIBRARY AND INFORMATION SCIENCE

Boss, Richard W. Telecommunications for Library Management.
White Plains, NY: Knowledge Industry Publications, Inc., 1985.

This discussion focuses on the changing needs of libraries in relation to data communications with much of the problems revolving around rising costs and emerging technologies. With a strong focus on cost-effectiveness, the following aspects of telecommunications are discussed: communicating concepts; standards; short-, medium-, and long-distance telecommunications; transmission suppliers; equipment; software products and how to actually procure products. The concept of "telecommunications literacy" is stressed for anyone involved with this technology especially in terms of initial procurement decisions.

Jacob, M.E.L. Telecommunications Networks: Issues and Trends.
White Plains, NY: Knowledge Industry Publications, Inc., 1986.

These articles were compiled by the American Society for Information Science (ASIS). The collection addresses the context of telecommunications issues and technology, OSI and the Linked Systems Project (LSP), and specific network perspectives including UTLAS and OCLC. This collection is replete with tables and figures which illustrate main points especially useful to the information professional in need of a general overview.

Learn, Larry L. Telecommunications for Information Specialists.
Dublin, Ohio: OCLC Online Computer Library Center, Inc., 1989.

All aspects of telecommunications, as related to the library and information professional, are covered here including the role of telecommunications, regulation, network technology, networks and networking, telecommunications infrastructure, recent developments within the public network, and future networking strategies. Little previous knowledge of the technology is necessary as the intent here is to provide the basic background necessary for enlightened understanding, decision-making, and planning with this popular technology. Nearly half of this publication is devoted to a thorough glossary, bibliography and study guide.

Telecommunications for Information Management and Transfer:
Proceedings of the First International Conference held at
Leicester Polytechnic, April 11, 1987, edited by Mel Collier.
Brookfield, VT: Gower Publishing Company, 1988.

The main focus of this text is on telecommunications and its management as its services expand within the library. The thirteen chapters cover information on LAN, WAN, satellite communications, interactive fiber-optic networks, cable systems, e-mail, and the technological development of modern information technology systems. Each chapter delves into the benefits and consequences of the various aspects of telecommunications as a manner of information management and delivery.

TELECOMMUNICATION POLICY

Dougan, Diana Lady. New Telecommunications Services: Let's Not Stack the Deck Against Them. Washington, D.C.: U.S. Department of State, Bureau of Public Affairs, Office of Public Communication, Editorial Division, 1988.

This is an address by Ambassador Diana Lady Dougan, U.S. Coordinator and Director, Bureau of International Communications and Information Policy, before the World Plan Meeting sponsored by the International Telecommunication Union (ITU), Lisbon, Portugal, February 3, 1988. The author offers some opinions on the global advance of communications by offering examples of current international technology innovations, with a specific focus on less industrialized countries. Noting the trend for more affordable and accessible technology to individuals and small groupings as well as large, she discusses computer networking, competition and some of the advances of international telecommunications organizations. By addressing the issues of how to effectively provide telecommunications services in an exploding technological environment, how to project telecommunications traffic forecasts, and the financing of these new facilities, this overview is especially valuable for all information professionals.

Emard, Jean-Paul. Information and Telecommunications: an Overview of Issues, Technologies, and Applications. Report for the Subcommittee on Science, Research, and Technology of the Committee on Science and Technology, U.S. House of Representatives, 97th Congress, 1st Session. By the Science Policy Research Division, Congressional Research Service, Library of Congress. Washington. D.C.: G.P.O., 1981.

This report examines the role of information and telecommunications technology in government and society by providing an overview discussion of the key subject areas. The document is divided into three parts, with two appendixes. Part one introduces the information age with an overview of

national and global information and telecommunications issues as well as an overview of the application areas. Part two addresses the technologies of information and communications including history, detailed technology of systems and sample telecommunication systems. Part three focuses on future trends in information and telecommunications. The appendixes include a table of contents to selected readings, and an index to selected readings, by the author. Overall, this series serves as a useful guide in the quickly-changing and emerging field of information and communications.

"Telecommunications." Bulletin of the American Society for Information Science 16 (June/July 1990).

The entire issue of this bimonthly publication is devoted to the impact of telecommunications as related to the information professional. There are eleven articles of special interest which include some of the following topics: national library networks, computer networks, telecommunications for academic libraries, Terabit lightwave networks, software technology, Radio Free Europe, telecommunications education, and a review of the First Marconi International Fellowship and Symposium on "Innovation in Telecommunications: Is it working?" Overall, it is a good introduction to recent issues, policies and innovations in telecommunications.

United States Committee on Government Operations. Subcommittee on Government Information and Individual Rights. International Data Flow: Hearings before a subcommittee of the Committee on Government Operations, House of Representatives. 96th Congress, 2nd Session, March 10, 13, 27 and April 21, 1980. Washington, D.C.: U.S. G.P.O., 1980.

These hearings address the public and business sectors' experiences in regards to problems of international data flow and how they feel the executive branch could best be organized to represent the interests of the United States. The topic is broadly defined at two levels: 1) the traditional issue of trade, involving tariffs and ordinary, economically motivated, nontariff trade barriers, and how 2) barriers to trade are emerging from Government information laws intended to serve very different purposes, such as the protection of personal privacy.

This volume includes formal statements by authorities representing a variety of public and business entities, a collection of letters and statements submitted for the record and appendixes which include a statement submitted for the record by the Assistant Secretary for International Economic Policy, Department of Commerce, letters submitted for the

record by government agencies and private sector enterprises, associations, etc., a report of "The 1979 World Administrative Radio Conference," and a selection of references on international data flow, which would be especially useful to the information professional.

United States Committee on Government Operations. Subcommittee on Government Information and Individual Rights. International Telecommunications and Information Policy: Hearings before a subcommittee of the Committee on Government Operations, House of Representatives. 97th Congress. 1st and 2nd Sessions, December 2, 1981 and April 29, 1982. Washington, D.C.: U.S. G.P.O., 1982.

These hearings note that trade in information technology and services ranks second, behind agriculture, in its net positive balance for the United States. Telecommunications and computer services are the backbone of international trade in services, the area of enterprise in which the United States currently competes most effectively and which promises to dominate trade in the future. The hearings address the fact that the unencumbered use of information technologies provides the means to communicate political and cultural, as well as economic, information among nations and how barriers to international communications and information flow are developing very rapidly. The resultant statements deal with successful enactments of telecommunication policy such as the implementation of the OECD privacy guidelines via the National Telecommunications and Information Administration. The second hearing focuses more on the policies of the Federal Communications Commission and the executive branch regarding the entry of foreign firms into the U.S. communications and information service markets.

This document is really a plea to the U.S. government to take a proactive role in monitoring the provision of information goods and services as a wide range of barriers to the international flow of information threaten not only the export of these high technology products, but all sectors of the economy.

United States Committee on Foreign Relations. Subcommittee on Arms Control, Oceans, International Operations, and Environment. International Communication and Information Policy: Hearings before the Subcommittee on Arms Control, Oceans, International Operations, and Environment of the Committee on Foreign Relations. United States Senate. 98th Congress. 1st Session, October 19 and 31, 1983. Washington, D.C.: U.S. G.P.O., 1983.

These hearings address the fact that political pressures to prevent, control, and tax the flow of information and

communications technology are intensifying around the world. Because of this, Americans need a clearer understanding of these developments and to insist upon consistent high-level attention by the U.S. Government. The hearings attempt to provide a better understanding of international communications policy by looking at the policies currently pursued by the U.S. Government and the interagency policies, the function and performance of the principal international organizations and forums in this area, the attitudes in other countries and governments toward communication and information and the basic agenda and timetable for decisions in the future. Testimony is included by various specialists in international telecommunications policy including policy-makers, providers of services and users of services. The appendix includes an interesting article which discusses and compares the issue of privacy and human rights in both the United States and Europe.

Yurow, Jane H. Issues in International Telecommunications Policy: a Sourcebook. Washington, D.C.: The George Washington University Division of Continuing Education Center for Telecommunication Studies, 1983.

This sourcebook covers the International Telecommunication Union regulatory environment, transborder data flow, telecommunications and trade policy and intellectual property. Other topics are covered nominally including national security, mass media, economic development and standards. Each chapter attempts to provide information on the international organizations, U.S. laws and regulations, significant treaties and agreements, and court decisions related to that subject as well as an annotated bibliography. The chapter on TDF includes an article by Robert F. Aldrich about emerging issues in TDF including economic restrictions, vulnerability issues, restrictions on personal data, and mass media restrictions. The remainder of the chapter provides U.S. laws and regulations, foreign laws and policies, treaties and agreements, relevant activities of key international organizations, key international transnational data networks, Executive branch interagency committees, public advisory committees to the United States government and a bibliography.

TELECOMMUNICATION STANDARDS

Henshall, John and Sandy Shaw. OSI Explained: End-to-End Computer Communication Standards. Chichester, England: Ellis Horwood Limited, 1988.

This book provides a description of how OSI works. Despite its technical nature, the ISO standards are presented in an easy-to-understand manner including the rules and

procedures computer systems must follow in order to support the OSI user applications. The framework of the ISO Seven-Layer Reference Model is included which is essential in understanding the harmonizing tactics of OSI.

Linked Systems: Papers Presented as a Program Session at the 112th Membership Meeting of the Association of Research Libraries on May 6, 1988 in Oakland, California, by the Association of Research Libraries. Washington, D.C.: Association of Research Libraries, 1988.

Although these papers are aimed at research library directors, the topic, how linked systems will affect library operations, is both timely and relevant to all library professionals. The papers include an overview of OSI, the connection between LSP and the library community, and the implications for libraries, especially regarding future operations and technological innovations. It includes a brief list of selected readings.

Open Systems Interconnection: the Communications Technology of the 1990's: Papers from the Pre-conference Seminar held at London, August 12-14, 1987, ed. by Christine H. Smith. Munchen: New York, etc.: K.G. Saur, 1988.

These pre-conference seminar papers, organized by the IFLA Section on Information Technology, are an extremely useful resource regarding the function and importance of international standards in an OSI application. Divided into four sessions, the following topics are covered: data interchange/state of the art of OSI, document creation for interchange, implementations of library application layer protocols, and future challenges. This up-to-date collection of papers serves as an excellent introduction to library applications of OSI, especially in its coverage of the connection between OSI and IFLA programs.

TRANSBORDER DATA FLOW

Bender, David R. "Transborder Data Flow: An Historical Review and Considerations." Special Libraries 79 (Summer 1988): 230-235.

A condensed history of TDF is presented noting the original issues of personal privacy, national sovereignty, and economic concerns and indicating the need to resolve current problems of TDF including equitable international policies and standardization of information technology. Greatest stress is placed on the need for creation of an international agreement

that will serve the needs of all nations and parties involved in TDF.

CELIM Conference. Freedom of Data Flows and EEC Law: Proceedings of 2nd CELIM Conference. Deventel, The Netherlands: Kluwer Law and Taxation Publishers, 1988.

This is a collection of articles presented by the CELIM association (the European Committee 'Lex Informatica Mercatoriaque') consisting of lawyers from all areas of training, working on many issues including business law, information science law and international law in the European context. Divided into two parts, the legal status of data and the status for data flows in EEC law, the articles cover varied aspects of information law, and, more specifically, freedom of data flows and: the nature of data, the vectors of data, and customs taxation. Though much of the material is aimed at the legal community, many of the articles are especially insightful for those with interests in information science law.

Dougan, Diana Lady. The High Stakes Game of International Standard Setting. Washington, D.C.: Department of State, Bureau of Public Affairs, Office of Public Communication, Editorial Division, 1987.

This is an address before a symposium on standards sponsored by the National Bureau of Standards. Dougan notes that standards include many international dimensions, involving a variety of sectors other than telecommunications ("the whole world of common carrier services, broadcast media, and computers"). Defining the various standards as 1) no standard at all, 2) de facto standard, 3) voluntary standard, and 4) the treaty-based standard, this address focuses on the latter two because they are the ones directly involving governments. By identifying problems and possible solutions, this address serves as an excellent overview of the process of standard-setting.

Dougan, Diana Lady. Promoting the Free Flow of Information. Washington, D.C.: U.S. Department of State, Bureau of Public Affairs, Office of Public Communication, Editorial Division, 1983.

This is an address by Ambassador Diana Lady Dougan, Coordinator International Communication and Information Policy, before the Second Symposium on Transborder Data Flows of the OECD, London, November 3, 1983. Dougan addresses how, in the field of telecommunications, change is so rapid and

that we must constantly adjust to its technological, legal, and economic implications. She stresses the United State's support of the OECD which has a valued and unique role in identifying and addressing the challenges of our future in information, computers and communications. Also mentioned is the Committee on Information, Computer and Communications Policy (ICCP) and the role it should take in this area, how to establish appropriate coordination mechanisms with other international organizations, and to develop a series of projects that reflect identified priorities.

Duchesne, Roddy. "IFLA Transborder Data Flow Survey." UDT Newsletter 2 (August 1987): 1-12.

This article describes a survey taken in 1986 by the International office for UDT, in connection with the National Library of Canada. The results of 104 respondents, from national libraries, national library associations and 12 other database service providers, with a response rate of 30%, are tabulated and discussed providing some of the most practical feedback concerning TDF as related to libraries. The article focuses not only on current issues but provides interesting suggestions, as stated by respondents, about the focus of future TDF-related issues, research, and pilot projects.

Global Ties through Information: Papers presented at the State-of-the Art Institute, October 17-19, 1988, Washington, D.C. Special Libraries Association: Washington, D.C., 1989.

This collection includes 16 various viewpoints of global information flow. The effects of TDF as it affects finance, economics, legislation, demographics, and world relations are discussed. In particular, the following topics are addressed: international communications and tensions over information networks, international satellite networks, data communications in the third world, Japanese online information flow, international collaboration, emergency management utilizing information technology, and definitions of major information technologies.

Hamelink, Cees J. Transnational Data Flows in the Information Age. Lund, Sweden: Studentlitteratur, 1984.

The author presents an overview of all aspects of international data transfer as of the mid-1980s. Focusing on the information age, telematics, data networks and data flows, the role of the transnational corporation, TDF and the third world, and data regulation, the author chooses to focus more on the political, economic and cultural impact of this

phenomenon. He stresses the need for technological advancement in order to broaden and standardize the transnational flow of data. It includes a bibliography and index.

Intergovernmental Bureau for Informatics (IBI). Transborder Data Flow Policies: Papers Presented at the IBI Conference on Transborder Data Flow Policies, Rome (Italy), 23-27 June 1980. New York: UNIPUB, 1980.

This collection of 35 papers covers a variety of TDF issues in English, Spanish, and French. It is useful because of its international nature and, historically, because many of the papers are the first documentation of TDF in certain regions of the world. The collection addresses not only legal, business and economic issues, but several areas of library and information science. Especially useful is an extensive TDF bibliography available from IBI.

International Federation of Library Associations Transborder Data Flow Program. Introductory TDF Study: Final Report. Ottawa, Canada: Locus Informatics, Inc., 1986.

This report is a result of the first year's work of the TDF Programme, including individual reports created at various stages during that year. The main focus of the TDF office, after its establishment in 1986, was the development of questionnaires and analysis of the responses. Secondary was to insure a second year program, to investigate electronic mail services and to establish a ten-year proposal. Included here is a status statement on these activities, along with appendixes more clearly detailing each of these activities.

This is an important document in that it is one the first to alert the IFLA community as to the existence of the program, for the responses received by respondents indicating priorities and activities which would be of benefit to members, and for the identification of current restrictions to TDF, as well as the quantification of the amount of TDF including current and future characteristics.

Jussawalla, Meheroo and Chee-Wah Cheah. The Calculus of International Communications: a Study in the Political Economy of Transborder Data Flows. Littleton, CO: Libraries Unlimited, Inc., 1987.

This discussion addresses many current issues of TDF, especially in regards to technological implications and their increasing importance versus issues of national sovereignty, and the freedom of information. The first section discusses

the problem of TDF including the nature and implications of TDF, the historical and institutional setting and the growth of the services section, in particular, the implications for trade policy. Part two addresses the new directions for economic analysis including analysis of the legal and policy aspects of information privacy, the economies of political choice and TDF regulation and elements of TDF economies. The conclusion summarizes the issues and includes a proposal for TDF policy coordination. It includes reference notes and an index.

Kent, Allen, ed. Encyclopedia of Library and Information Science Vol. 45, Supp. 10. New York: Marcel Dekker, Inc., 1990. S.v. "Transborder Data Flow," by Roddy Duchesne and Anna Levin.

This article covers most aspects of TDF as related to libraries. Much of the findings are based on the results of the IFLA Survey taken in 1986 under the guise of the UDT Program. The results are detailed under the categories of library applications, modes of transmission, geographical distribution, barriers to TDF, and significance of TDF. Noting that involvement of libraries in TDF is limited, the fact that increased involvement is stressed as well as the need for further attention to the content of communication and the purpose which it serves. National governments' involvement with TDF is discussed regarding national, economic, cultural and technological sovereignty, security, and lesser developed countries. Further discussion focuses on corporations, the information industry and private individuals, each struggling with particular TDF issues.

Kirsch, William. Transborder Data Flows: a Current Review. London: International Institute of Communications, 1983.

This review discusses TDF by breaking it into two broad categories, those being TDF of personal data and TDF of non-personal data. The rationale for this division is that early activity focused on issues of personal data flow with more recent focus on non-personal data, especially with the increase in international databases. This guide discusses privacy, data protection and free flow of information and national sovereignty, developed and developing countries, international organizations and the selected issues of: remote sensing, electronic funds transfer and employment.

Maruyama, Lenore S. Transborder Flow of Bibliographic Data. IFLA Professional Reports: 7. The Hague: IFLA Headquarters, 1985.

Initiated by the IFLA Section on Information Technology

in 1983, this study aims to investigate any barriers to the flow of bibliographic information and to make proposals for solutions and actions. Because the interconnection of data bases between nations is so important, the library and information professions need to be aware of anything that would affect the free flow of information. A discussion of the flow of bibliographic data focuses on major participants, present and estimated future flow of data, a comparison of international circulation of other types of data, and the barriers to flow of bibliographic data. The paper closes with a list of proposals for actions as well as with an appendix of trade barriers to telecommunications, data, and information services. Though much information of this sort is quickly out-dated, this paper is a useful tool regarding the history of TDF and its connection with the library and information professions.

United Nations Centre on Transnational Corporations. Transborder Data Flows: Transnational Corporations and Remote-Sensing Data. 1984.

This document focuses specifically on remote-sensing which is a unique form of TDF in that it not only permits the transmission of data between countries, but also makes it possible to generate new data about particular countries and disseminate this data elsewhere. Remote-sensing is related to transnational corporations due to the enhanced data-collecting techniques and how it is used in operational terms. Included here is an introduction to remote-sensing and a review of national remote-sensing programs, as well as a discussion of obstacles to the use of remote-sensing and a review of policy and regulations. Understanding of this technology is useful for those involved in the use of satellite-acquired remotely-sensed data for negotiations between various parties.

Universal Dataflow and Telecommunications (UDT) Newsletter. Ottawa, Canada: IFLA International Program for UDT, No. 1, 1987-

This irregular newsletter (English and French) is published by the Universal Dataflow and Telecommunications Core Program of IFLA. Its chief aim is to inform members of the IFLA community about international activities and developments which concern the program. Each issue contains various topics via the 'Update' and 'Focus on OSI' sections. Other relevant issues are often the topic of an entire newsletter. This is one of the most authoritative sources on current trends in TDF.

APPENDIX ONE

Guidelines on the Protection
of Privacy and Transborder Flows
of Personal Data

Source: Organization for Economic Cooperation and Development.
Guidelines on the Protections of Privacy and Transborder
Flows of Personal Data. (Paris: OECD, 1981), 9-36.

**RECOMMENDATION OF THE COUNCIL
CONCERNING GUIDELINES GOVERNING THE PROTECTION
OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA**
(23rd September, 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data.

That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
 - a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
 - b) "personal data" means any information relating to an identified or identifiable individual (data subject);
 - c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
 - a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
 - b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
 - c) the application of the Guidelines only to automatic processing of personal data.

Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- a) as few as possible, and
 - b) made known to the public.
5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.
6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
 - i) within a reasonable time;
 - ii) at a charge, if any, that is not excessive;
 - iii) in a reasonable manner; and
 - iv) in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes

specific regulations in view of the nature of those data and for which the Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- a) adopt appropriate domestic legislation;
- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

PART FIVE INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

- i) information exchange related to these Guidelines, and
- ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

EXPLANATORY MEMORANDUM

INTRODUCTION

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.

The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions.

The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

Activities at national level

4. Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk of "data laws" or "data protection laws" (lois sur la protection des données) whereas in English speaking countries they are usually known as "data protection laws". Most of the statutes were enacted after 1973 and the present period may be described as one of continued or even widening legislative activity. Countries which already have statutes in force are to be found in new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and papers prepared by public committees or similar bodies, help to bring attention to the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

5. The approaches to protection of privacy and individual liberties used by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data held for their use; the identification of parties who are responsible for compliance with the relevant privacy protection rules and procedures. Generally speaking, statutes to protect privacy and individual liberties relate to personal data attempt to cover the successive stages of the data process beginning with the initial collection of data and ending with eradication of similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

6. Differences between national approaches as apparent at present in laws, bills or proposals for legislation refer to aspects such as the scope of legislation, the emphasis placed on different elements of protective machinery of enforcement. Thus, opinions vary with respect to the requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing trade differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

I. GENERAL BACKGROUND

The Problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

International aspects of privacy and data banks

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.
8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.
9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

Relevant international activities

10. There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at international co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).
11. A number of international agreements deal in a more general way with the issues which are at present under discussion, viz. the protection of privacy and the free dissemination of information. They include the European Convention of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).
12. However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

13. In 1973 and 1974 the Committee of Ministers of the Council of Europe adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

14. Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks and rules of conduct for data processing professionals. The Convention was adopted by the Committee of Ministers on 17th September 1980. It seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

15. The European Community has carried out studies concerning the problems of harmonization of national legislations within the Community in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

Activities of the OECD

16. The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, e.g. in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.
17. A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised (a) the need for generally continuous and uninterrupted flows of information between countries, (b) the legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens, (c) the economic value of information and the importance of protecting "data trade" by accepted rules of fair competition, (d) the needs for security

guards to minimise violations of proprietary data and misuse of personal information, and (e) the significance of a commitment of countries to a set of core principles for the protection of personal information.

18. Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an international Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by 1st July, 1979.

19. The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

a) The specific, sensitive facts issue

The question arose as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (e.g. credit reporting). Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.

b) The ADP issue

The argument that ADP is the main cause for concern is doubtful and, indeed, contested.

c) The legal persons issue

Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.

d) The remedies and sanctions issue

The approaches to control mechanisms vary considerably: for instance, schemes involving supervision and licensing by specially constituted authorities might be compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.

e) The basic machinery or implementation issue

The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or

objectives and lower level "machinery" questions which should be left to domestic implementation.

f) The choice of law issue

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of transborder data flows. The question arose, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.

g) The exceptions issue

Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?

h) The bias issue

Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

20. During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organisations; thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a convention which will be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

21. The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

II. THE GUIDELINES

A. PURPOSE AND SCOPE

General

22. The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries.

24. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

25. The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

- a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;
- b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;
- c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and
- d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder

flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

26. Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

- a) effective national measures for the protection of privacy and individual liberties;
- b) avoidance of practices involving unfair discrimination between individuals; and
- c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-Member countries

28. The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-Member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-Member countries and appropriate international organisations.

The broader regulatory perspective

29. It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments governing such issues

human rights, telecommunications, international trade, copyright, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

30. Some Member countries have emphasized the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

31. Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

32. Similarly, it is debatable to what extent people belonging to a particular group (e.g. mentally disabled persons, immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

33. On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated in the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (cf. paragraph 49 below).

Automated and non-automated data

34. In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and computer networks. The Expert Groups has devoted special attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by

automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

35. On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, "mixed" data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or micro-computers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

36. Because of the difficulties mentioned, the Guidelines do not put forward a definition of "automatic data processing" although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

37. Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

38. It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes. It should be emphasized that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

B. DETAILED COMMENTS

General

39. The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

40. The list of definitions has been kept short. The term "data controller" is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, viz. (a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes; (b) data processing service bureaux which carry out data processing on behalf of others; (c) telecommunications authorities and similar bodies which act as mere conduits; and (d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities. Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

41. The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.

42. The term "transborder flows of personal data" restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

43. The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, viz. that data pose a danger to privacy and individual liberties. Such dangers can

arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

44. As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3(b) provides for many "trivial" cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3(c) provides for such a limitation.

Paragraph 4: Exceptions to the Guidelines

46. To provide formally for exceptions in Guidelines which are part of a non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (e.g. through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret.

he formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions — hence the wording that they include national sovereignty, national security and public policy (“ordre public”). Another overriding national concern would be, for instance, the financial interests of the State (“crédit public”). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, e.g. the regulation of certain types of data or activities as compared to regulation of a general nature (“omnibus approach”).

47. The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

48. In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

49. First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection Limitation Principle

50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed

in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, viz. (a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal records; for instance). On the other hand, it may be held that no data are intrinsically “private” or “sensitive” but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

51. The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. If or one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to:

- data quality aspects (i.e. that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.);
- limits associated with the purpose of the processing of data (i.e. that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose);
- “earmarking” of specially sensitive data according to traditions and attitudes in each Member country;
- limits to data collection activities of certain data controllers;
- civil rights concerns.

52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder (“where appropriate”) that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled person, etc.

Paragraph 8: Data Quality Principle

53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose Specification Principle

54. The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time of data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest: this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use Limitation Principle

55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative - see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security Safeguards Principle

56. Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasized that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has a broad coverage. The cases mentioned in the provision are to some extent overlapping (e.g. access/disclosure). "Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. "Modified" should be construed to cover unauthorised input of data, and "use" to cover unauthorised copying.

Paragraph 12: Openness Principle

57. The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual Participation Principle

58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual subparagraphs, the following explanations are called for:

59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from

situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.

60. The right to reasons in Paragraph 13(c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, e.g. in order to inform and alert a subject to his rights so that he can exercise them effectively.

61. The right to challenge in 13(c) and (d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.); such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability Principle

62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. Paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic Principles of International Application

63. The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with

security issues in a broad sense and may be said to correspond, at the international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, i.e. effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

64. For domestic processing Paragraph 15 has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

65. Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (e.g. access to the addresses of nationals living abroad).

66. As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to Paragraph 16, be uninterrupted and secure, i.e. protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, i.e. data which pass through a Member country without being used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that convention, the members of the International Telecommunications Union, including the OECD Member countries, have agreed, inter alia, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international telecommunications. As regards exceptions, the right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws on the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines in

their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

67. Paragraph 17 reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned - in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, Paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

68. Paragraph 18 attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus not openly announced. However, Paragraph 18 is not intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for international data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National Implementation

69. The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect. The opening sentence shows the "different approaches which might be taken by countries, both generally and with respect to control mechanisms (e.g. specially set up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

70. In Paragraph 19(a) countries are invited to adopt appropriate domestic legislation, the word "appropriate" foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions. Paragraph 19(b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19(c) should be given a broad interpretation, it includes such means as advice from data controller, and

the provision of assistance, including legal aid. Paragraph 19(d) permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19(e) dealing with discrimination is directed against unfair practices but leaves open the possibility of "benign discrimination" to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information Exchange and Compatible Procedures

71. Two major problems are dealt with here, viz. (a) the need to ensure that information can be obtained about rules, regulations, decisions, etc. which implement the Guidelines, and (b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

72. The importance of the second problem is, generally speaking, proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for coordinating special provisions on transborder data flows in domestic laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for Co-operation

73. The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21(ii), i.e. mutual aid in procedural matters and requests for information, is future-oriented: its practical significance is likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of Laws

74. The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a

theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

75. As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

76. In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

77. The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.

APPENDIX TWO

Convention for the Protection of Individuals
with Regard to Automatic Processing of
Personal Data

Source: Pipe, Russell. A Business Guide to Privacy and Data Protection Legislation. (Paris: ICC Publishing S.A., 1981), 344-352.

COUNCIL
OF EUROPE



CONVENTION FOR THE PROTECTION OF INDIVIDUALS
WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA

PREAMBLE

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms ;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy; taking account of the increasing flow across frontiers of personal data undergoing automatic processing ;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers ;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows :

CHAPTER I — GENERAL PROVISIONS

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

Definitions

For the purposes of this convention :

a. "personal data" means any information relating to an identified or identifiable individual ("data subject") ;

b. "automated data file" means any set of data undergoing automatic processing ;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means : storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination ;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.
2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe :
 - a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law ;
 - b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality ;
 - c. that it will also apply this convention to personal data files which are not processed automatically.
3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.
4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.
5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.
6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II — BASIC PRINCIPLES FOR DATA PROTECTION

Article 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.
2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5
Quality of data

Personal data undergoing automatic processing shall be :

- a. obtained and processed fairly and lawfully ;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes ;
- c. adequate, relevant and not excessive in relation to the purposes for which they are stored ;
- d. accurate and, where necessary, kept up to date ;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6
Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7
Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8
Additional safeguards for the data subject

Any person shall be enabled :

- a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file ;
- b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form ;
- c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention ;
- d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9
Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of :

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences ;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs *b*, *c* and *d*, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11

Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

CHAPTER III — TRANSBORDER DATA FLOWS

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2 :

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection ;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

CHAPTER IV — MUTUAL ASSISTANCE

Article 13

Co-operation between Parties

1. The Parties agree to render each other mutual assistance in order to implement this convention.
2. For that purpose :
 - a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe ;
 - b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.
3. An authority designated by a Party shall at the request of an authority designated by another Party :
 - a. furnish information on its law and administrative practice in the field of data protection ;
 - b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14

Assistance to data subjects resident abroad

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.
2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.
3. The request for assistance shall contain all the necessary particulars, relating *inter alia* to :
 - a. the name, address and any other relevant particulars identifying the person making the request ;
 - b. the automated personal data file to which the request pertains, or its controller ;
 - c. the purpose of the request.

Article 15

Safeguards concerning assistance rendered by designated authorities

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.
2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16

Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless :

- a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying ;
- b. the request does not comply with the provisions of this convention ;
- c. compliance with the request would be incompatible with the sovereignty, security or public policy (*ordre public*) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17

Costs and procedures of assistance

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.
2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.
3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

CHAPTER V — CONSULTATIVE COMMITTEE

Article 18

Composition of the committee

1. A Consultative Committee shall be set up after the entry into force of this convention.
2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.
3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

Article 19

Functions of the committee

The Consultative Committee :

- a. may make proposals with a view to facilitating or improving the application of the convention ;

b. may make proposals for amendment of this convention in accordance with Article 21 ;

c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3 ;

d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

Article 20

Procedure

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.
2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.
3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.
4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

CHAPTER VI — AMENDMENTS

Article 21

Amendments

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.
2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.
3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.
4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.
5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.
6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

CHAPTER VII — FINAL CLAUSES

Article 22

Entry into force

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.
3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

Article 23

Accession by non-member States

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.
2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24

Territorial clause

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.
2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.
3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25

Reservations

No reservation may be made in respect of the provisions of this convention.

Article 26

Denunciation

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27

Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of :

- a. any signature ;
- b. the deposit of any instrument of ratification, acceptance, approval or accession ;
- c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24 ;
- d. any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each of the signatory and acceding States.