LEGAL ASPECTS OF TRANSBORDER DATA FLOWS AND PROTECTION OF PRIVACY: Contemporary Developments in Establishing Legal Regimes over a Rapidly Emerging Field of Telematics

by

Ikuko OTA

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Master of Laws.

INSTITUTE OF COMPARATEIVE LAW
McGILL University
Montreal, Quebec
CANADA

September 1990

ABSTRACT

The purpose of this thesis is to clarify what the international regulatory techniques governing Transborder Data Flows (TDF) should be. This thesis deals mainly with the concepts and implementation of rules relating to the protection of privacy and transborder flows of personal data, as adopted by two international organizations, namely the OECD and the Council of Europe. The focus of this study is on the influence of two instruments adopted in 1980, (namely the OECD Guidelines and the CoE Convention,) on the national data protection policies of the member states. A further section is devoted to reviewing their impact on Japanese public and private sectors.

Employing the findings arising from the activities of these two organizations, the concluding chapter links the theoretical and empirical components of the study to indicate certain conditions necessary for establishing an effective legal regime over a rapidly emerging field of telematics.

RÉSUMÉ

Le but de cette thèse est de clarifier ce que devraient être les techniques régulatrices régissant les flux transfrontières de données. La presente thèse traite principalement des concepts et de l'exécution des regles concernant la protection de la vie privée et des flux transfrontières de données à caractère personnel, telles qu'adoptées par deux organisations internationales, a savoir l'OCDE et le Conseil de l'Europe (le Conseil). Cette étude se focalise sur l'influence de deux instruments adoptés en 1980, a savoir les Recommandations de l'OCDE et la Convention du Conseil, sur la politique des Ftats membres concernant la protection nationale des données. En outre une section est consacrée a la revue de leur impact sur les secteurs prive et publique Japonais.

Enfin, en employant les constatations qui ressortent des activités des deux organisations précitées, le chapitre concluant renoue les composantes théoriques et empiriques de la présente étude afin d'indiquer certaines conditions nécessaires pour établir un régime légal efficace relatif à la télématique, une discipline en rapide croissance.

ACKNOWLEDGEMENTS

During the preparation of this thesis, I have received much support and encouragement in both Canada and Japan.

Among the people at McGill University whose support I would particularly like to mention, to my thesis supervisor, Dr. R. S. Jakhu (Assistant Director, Center for Research of Air and Space Law), I wish to express my sincere gratitude for his constant encouragement and his generous gift of time and advice throughout my extended Master's Program of 1986-90. Furthermore, my special thanks are due to Prof. W. Graham (European Community Law) who gave me a dynamic and practical concept of "law" in transnational activities among nation-states. Prof. A. de Mestral (Director of Institute of Comparative Law), Prof. M. Bridge (the acting Director of 1986-87), and Prof. N. M Matte (Director of Center for Research of Air and Space Law), very kindly provided at all times a fruitful environment for my study and research in Montreal. I am also grateful to Mrs. G. Van Leynseele (Graduate Programs Coordinator, Institute of Comparative Law), for her warm encouragement and special advice and help regarding my coursework and research during 1986-1990.

Much of the research and writing for this thesis was carried out in Japan since 1987 as a graduate law student of Hitotsubashi University, Tokyo.

In Tokyo, I am especially indebted to Mr. M Muramatsu (Director for International Planning and Research Management and Coordination Agency, Government of Japan), and Mr. K. Nanba (Second International Organization Division, Economic Affairs Bureau Ministry of Foreign Affairs, Government of Japan) for their kind granting of interviews and valuable suggestions regarding the practices of both the OECD and Japan in the field of transborder flows of personal data.

At the Graduate School of Law, Hitotsubashi University, Prof. T. Kuwabara, Prof. Y. Otani (Public International Law), Assoc. Prof. T. Sato. (International Organizations Law), Prof. M. Horibe (Informatics Law) and Prof. J. Akiba (Private International Law), always gave generous support and much time to comment on my research and writing. I also wish to express thanks to Mr. R. Ford and Ms. J. Cauwenbergh, graduate law students of Hitotsubashi University, for their help in the tedious work of correcting the grammatical errors in the manuscripts.

The research on which this thesis is based was supported by the 1989-1991 Fellowship of Japan Society for the Promotion of Science and the 1989-1991 Grant for Special Research of the Japanese Ministry of Education (Grant No. 01790122). I am also grateful for the following grants namely the 1986-87 Rotary Foundation Academic Scholarship, the Special Awards by Institute of Comparative Law (Fall-term 1986-87) and the Foreign Student Fee-Waiver (Summer session of 1987) by McGill University, without such economic support the completion of the Master's Program coursework would not have been possible.

TABLE OF CONTENTS

INTRODUCTION.

Objective, Focus of this Thesis, and Method of Research

It was in the sphere of protection of privacy and personal data*1 that, the phenomenon that came to be known as "Transborder Data Flows" (hereinafter TDF) first gave rise to international concern.

Responding to this issue, on 17 September 1980, the Council of Europe (hereinafter the CoE) adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*2 (hereinafter the CoE Convention). Yet, at almost the same time, another international organization, the Organization for Economic Co-operation and Development (hereinafter the OECD), eighteen of whose member states also belong to the CoE*3, adopted an instrument on the same subject: on 23 September 1980. it adopted the Recommendation of the OECD Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*4 (hereinafter the OECD Guidelines),

From these facts, some questions can be asked.

1. Given the overlap in membership of the two organizations, why were two instruments needed on the same subject?
2. Are there any differences between the two instruments?
3. What is the significance of the difference in the forms of the two instruments, namely the recommendation and

the convention?

All these questions will be approached along with the overall problem of what the international regulatory techniques governing TDF, being one of the rapidly emerging field of telematics*5, should be. The objective of this thesis is to find a solution to this problem.

This thesis deals mainly with the legal regime relating to the protection of privacy and transborder flows of personal data, because to date, it is this field among all TDF-associated problems which provides the greatest quantity of materials for examination, at both international and national level. The focus of this study is on the influence of the OECD Guidelines and the CoE Convention on the national data protection policies of the member states.

In the presentation, Chapter 1 takes a general view of the issues involving TDF, and defines the term "TDF" for the purpose of this study. Chapter 2 analyzes national laws and policies concerning data protection, with emphasis on the different approaches taken by the U.S. and Europe, at the time the OECD and the CoE adopted their respective rules in 1980. Chapter 3 consists of a comparative examination of the measures taken by the the OECD and the CoE towards the harmonization of data protection laws. In Chapter 4, the achievements of the two international organizations are evaluated, and compared to the analysis results in Chapter 2. A further section is

devoted to reviewing their impact on Japanese public and private sectors. Finally, employing the findings made in the preceding chapters, Chapter 5 links the theoretical and empirical components of the study to indicate certain conditions considered necessary for establishing an effective legal regime over a rapidly emerging field of telematics.

Footnotes to INTRODUCTION

*1 "Personal data" means any information relating to an identified or identifiable individual (data subject) [the OECD Guidelines para. 1(b), the CoE Convention art. 2(a)].

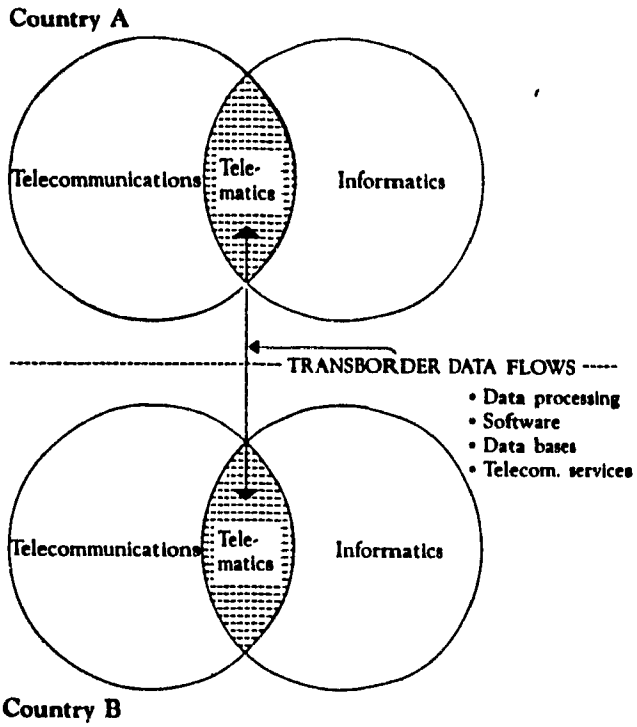
*2 28 January 1981, E.T.S. No.108, reprinted in 20 I.L.M. 317. The text of the CoE Convention is contained in ANNEX 2 of this thesis.

*3 Austria, Belgium, Denmark, France, Federal Republic of Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. Since in May 1989 Finland acceded to the Council of Europe, as of April 1990, nineteen member states are overlapped between the OECD and the CoE.

*4 OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris. OECD, 1981) at 7-12 [hereinafter The OECD Guidelines]. The text of the OECD Guidelines is contained in ANNEX 1 of this thesis.

*5 "Telematics" means the phenomenon which is the result of the merger of telecommunications and informatics, i.e. the study and/or the phenomenon of how data are processed and transmitted through digital-processing equipment. See Figure 1 [reproduced from. K.P. Sauvant, International Transactions in Services: The Politics of Transborder Data Flows (Boulder, Colo.: Westview Press, 1986) at 6]. See also Chapter 1 [sec. 1.2.1] of this thesis.

Figure 1. Telecommunications, informatics, telematics, and TDF



CHAPTER 1.

Transborder Data Flows:
An Overview of the Issues Involved

1.1 Defining the Term "TDF"

1.1.1 Origin of the Term "TDF"

The origin of the term "TDF" can be traced back to a seminar on privacy protection held in June 1974 by the OECD. There the term was used at an international level for the first time. And in the seminar, the possibility of danger was pointed out, that national data protection laws would be circumvented if data concerning its nationals were transfered and held in computers located in other countries having data protection laws with lenient standards or none at all*1.

Since then, the expression TDF has been given a variety of definitions by policy-makers within the private sectors and the academic world*2. For example, W. Fishman speaks of "electronic movement of data between countries*3". E. Novotny discusses "units of information coded electronically for processing by one or more digital computers which transfer or process the information in more than one nation-state*4". Pool and Solomon refer to "computer communications, telecommunications networks. .[d]igitalized transmission

enab[ling] voice and data traffic to be handled in a single mixed stream of data*5."

For the purposes of the OECD Guidelines, the term "transborder flows of personal data" was defined in paragraph 1 (C) as "movements of personal data across national borders".

On the other hand, in the CoE Convention, after defining "automatic processing", for the purposes of the Convention, as including "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" [art. 2(c)], Article 12(1) provides:

> 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.

1.1.2 Definition of TDF in this Thesis

However, the following two elements can be pointed out as being common to the various definitions of TDF.

Firstly, TDF is an international phenomenon based on

"telematics", which is the product of the merger of telecommunications and informatics*6. Neither the OECD Guidelines nor the CoE Convention defines strictly the medium of TDF or the means of data transmission, except to state that TDF includes the transmission of data by satellite*7 and physical transport of magnetic tapes or discs*8. Secondly, to be identified as TDF, its technical process has to be comprised of transmission, storage, and computation*9.

Therefore, for the purpose of this thesis, TDF should be understood as "a transnational phenomenon of exchange of information whose transmission, storage, computer-processing are undertaken by the merger of telecommunications and informatics"*10.

1.2 Issues and Concerns surrounding TDF

1.2.1 Understanding TDF in the Context of the "Information Revolution"

The concept of the "information society" is used almost universally to identify the new social and economic environment brought about by the new technologies which have arisen over the past two decades. Until recently, the societies of the advanced nations largely revolved around the production, distribution, and consumption of "goods". However, since the

1960s, because of the proliferation of computers in advanced societies and innovation in new and high technology in recent years, the significance of "information" in human activities has been increasing drastically. In other words, whereas the proportion of labor accounting for the production of "goods" has decreased greatly, the production, transfer, and use of "information" is fast becoming the focus of life and society. Moreover, because of this technological innovation, movements of people, goods, services, and money beyond national borders are integrating rapidly. The present situation we are faced with is, therefore, not an evolutionary one but something entirely new, namely the "information revolution".

Under this information revolution, many established institutions, national and international, can not adapt to rapid changes and major shifts in policy. The main reason for this institutional inability originates from a concept that the information revolution consists of convergences. The convergences are occurring in at least three dimensions, namely conduit/content in communications technology and industry, law/economics and nationality/internationality in telecommunications policy*11.

The traditional regulatory regime governing international telecommunications, established by the International Telecommunication Union (ITU), coordinated national telecommunications systems and integrated them into global

networks. Because of a synthesis of the legal and technical characteristics, the regime has succeeded well in avoiding conflicts arising from extraterritorial applications of national laws. From an economical viewpoint, it has preserved national economic prerogatives on the basis of reciprocity, or mutual recognition of territorial control over national systems. However, the emergence of telematics, or the interdependence of telecommunications and informatics, with the proliferation of international networks, changed the situation in a revolutionary manner. The convergence of conduit and content in communications technology brings about the overlapping of the carriers of conduit and the producers of content. Telecommunications networks gradually evolve from separate ones offering specific telecommunications services, into integrated ones, offering every possible telecommunications service, i.e. "integrated services digital network" (ISDN). Along with the degree of internationalization brought about by international computer networks international integration of industries and industrial operations has increased. As a matter of international economics, sovereign autonomy based on territoriality is no longer superior to other nations' policies of deregulation or privatization for the industries concerned. These trends lead to the convergences of law and economics, and nationality and internationality in telecommunications policy.

Hence, when TDF is considered in the context of the "information revolution", the concepts of convergence and rapid-responsiveness seem to be essential to a discussion on the legal rules concerning TDF. The concept of convergence requires a new integrated regulatory instrument which has traditionally been separated into different categories, such as telecommunications law, the law of broadcasting, data protection law. The concept of rapid-responsiveness needs a new regulatory institution without the old rigid structures and perceptions, which can deal adequately with changing legal requirements.

1.2.2 Emergence of "TDF Problems"

In this "information society", information itself, rather than physical resources, come to possess a greater economic value, especially in the context of international business transactions. Therefore, the advantages gained from increased quantity of data stored, from improved processing technology, and from enhanced data usage, will largely decide which players on the international scene will gain predominance. In the latter half of the 1970s, this predominance seemed to be taken by the United States, given the U.S.'s domination in both the software and hardware markets and international data services*12.

Recognizing the U.S 's predominance as a threat to national autonomy, other developed Western nations began to review their policies concerning telematics. Sweden, for example, fearing greatly the vulnerability of its society due to its inability to control or protect data concerning its nationals stored in foreign states, sought to establish its information sovereignty*13. Countries like Canada*14 and France*15 immediately understood TDF as an economic issue that has both positive and negative effects on the growing industry concerned and on national development as a whole. Member countries of the European Community (EC) considered themselves to be too small to develop the telematics potential within the their own national boundaries, and started to take joint action, including the building of a regional network system "EURONET", to link their economies to compete more effectively*16. Feeling insecure about its dependence on the U. S. data bases, Japan also started some studies*17 about the opportunity and potential of a huge telematics marketplace and enhanced economic growth arising therefrom, but it failed to provide a comprehensive political strategy for dealing with TDF per se.

Following this period of reviews, various states adopted individual telematics policies, which, when exposed to market forces in the international telecommunications sector, were subjected to a certain degree of competition of a Darwinian

nature. Despite this, three fields were seen to be common to all these pieces of national policies, namely

1. the protection of rights concerning privacy and intellectual property rights,
2. the preservation of national security and cultural identity,
3. the development of national economy and telematics industory.

Because of TDF's special characteristics of convergence and rapid-change, which have already been observed above, it may not be possible to draw distinct lines of demarcation among various difficulties arising from TDF. Thus it would be hard to describe every single issue of TDF problems separately, such as privacy protection, computer crime and fraud, liability for loss and error in data transmission, applicable law, intellectual property rights on software and data bases, authentication and evidential value of computer records, and trade secret.

However, we can at least recognize the term "TDF problems " as applying to various confrontations and contradictions that the differences of national policies and interests concerning TDF brought about. Therefore, what all TDF problems have in common is that an issue is caused by a confrontation between two competing forces, i.e. regulating and de-regulating TDF*18.

Footnotes to CHAPTER 1

*1 OECD, Transborder Data Flows: An overview of Issues, Note by the OECD Secretariat/ICCP Division. OECD Doc. DSTI/ICCP/83.29 (1983) at 3. This OECD document was publicly released at the Second OECD Symposium on TDF in London, 30 November - 2 December 1983.

*2 For a review of these various definitions of TDF, see A.W. Branscomb, "Global Governance of Global Networks: A survey of Transborder Data Flow in transition" (1983) 36 Vand. L. Rev. 985 at 990-993.

*3 W.L. Fishman, "Introduction to Transborder Data Flows" (1980) 16 Stan. J. Int'l L. 1 at 1.

*4 E.J. Novotny, "Transborder Data Flows and International Law. A policy-oriented framework of inquiry" (1980) 16 Stan. J. Int'l L. 142 at 143-144.

*5 I. Pool & R.J. Solomon, "Intellectual Property and Transborder Data Flows" (1980) 16 Stan. J. Int'l L. 113 at 114-115.

*6 See supra, INTRODUCTION note 5.

*7 The OECD Guidelines, supra, INTRODUCTION note 4 at 26 (para. 42).

*8 Council of Europe, "Draft Explanatory Report on the Draft Convention" (1980) 19 I.L.M. 299 at 312 (para. 56).

*9 E.J. Novotny, "Transborder Data Flow Regulation: Technical issues of legal concern" (Spring 1982) 3 Computer/L. J. 105 at 106.

*10 In 1985, the Declaration on Transborder Data Flows [11 April 1985, PRESS/A(85)30, reprinted in: "OECD Declaration on Transborder Data Flows" (1985) 8 T.D.R. 116 [hereinafter TDF Declaration]], the first multilaterally agreed instrument dealing specifically with the transborder flow of non-personal

data, was adopted by the OECD. Since then, a new trend of TDF definitions has emerged which attempted to understand TDF as trade in data services rather than solely on the "flow" per se. See, for example, P. Robinson, "Law Enforcement and Trade in Data Services" (December 1987) 10 T.D.R. 15 at 15. However, as this thesis deals mainly with the legal regime relating to the protection of privacy and transborder flows of personal data, the term TDF for this thesis is defined as such.

*11 See. E.-J. Mestmacker ed., The Law and Economics of Transborder Telecommunications (Baden-Baden: Nomos Verlagsgesellschaft, 1987) Part I· Introduction.

*12 "Telecommunications and computer goods and services account for the largest single share of the U. S. exports after agricultural products. The world market for telecommunications and information services was in excess of $130 billion in 1980, with the U. S. market accounting for 40% of that total." Quoted from: D. Yarn, "The Development of Canadian Law on Transborder Data Flow" (1983) 13 Ga. J. Int'l & Comp. L. 825 at 829 note 19.

*13 See, Sweden, Committee on the Vulnerability of Computer Systems, Ministry of Defense, The Vulnerability of the Computerized Society (Stockholm LiberForlag, 1979).

*14 See, Canada, Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty, Department of Communications, Telecommunications and Canadian Sovereignty [the so-called "Clyne Report"] (Ottawa Minister of Supply and Services, 1979)· see also, Yarn, supra, note 12.

*15 See, S. Nora & A. Minc, The Computerization of Society A Report to the President of France [the so-called " Nora & Minc Report"] (Cambridge, Ma.: Massachusetts Institute of Technology Press 1980).

*16 See, European Parliament, Report Drawn up on Behalf of the

Legal Affairs Committee on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing [the so-called "Bayerl Report"] Eur. Parl. Doc. (No.100/79) PE 56.386/fin. ; see also, T.J. Ramsey, "Europe Responds to the Challenge of the New Information Technologies: A teleinformatics strategy for the 1980s" (1981) 14 Cornell Int'l L. J. 237 at 283-284.

*17 Research Institute of Telecommunications and Economics, Prospects of the Demand for Data Communication (Research Institute of Telecommunications and Economics [Tokyo, Japan], 1977) [unpublished].

*18 For an overview of the TDF problems, see Figure 2 [reproduced from: W.J. Durka, "Legal Issues of Transborder Data Transmission" 74 Am. Soc'y Int'l. L. Proc. 175 at 178] and Table 1 [reproduced from: (1983) 6 T.D.R. 309] below. For a detailed study on specific TDF problems, see, OECD, An Exploration of Legal Issues in Information and Communication Technologies, OECD/ICCP Series No.8, (Paris: OECD, 1984); see also, The United Nations Commission on International Trade Law (UNCITRAL), The Legal Implications of Automatic Data Processing U.N. Doc. A/CN.9/279 (1986).

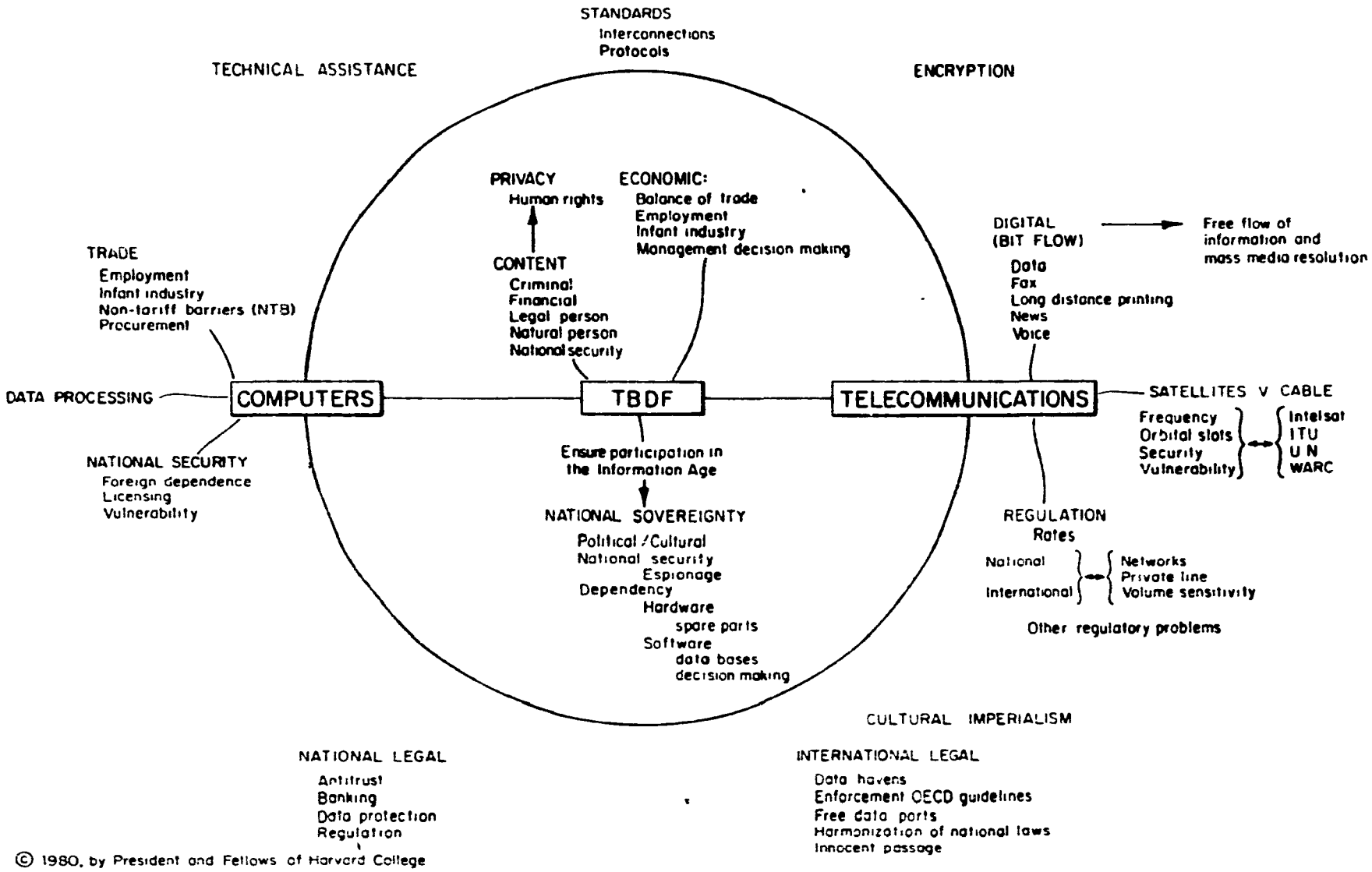


Figure 2. Overview of the "TDF Problems"

Table 1.

Overview of national and international bodies dealing with different TDF aspects

General aspects	*National*	*International*
Technical	Post and telecommunication authorities National standard bodies Hardware/software producers National trade facilitation bodies	International Telecommunication Union (ITU) Consultative Committee on Telephone and Telegraph (CCITT) International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) United Nations Economic Commission for Europe (ECE)
Political/ cultural	Departments of foreign affairs Department of education Radio and television authorities	United Nations General Assembly (UNGA) United Nations Economic and Social Council (ECOSOC) United Nations Educational, Scientific and Cultural Organization (UNESCO) Intergovernmental Bureau for Informatics (IBI)
Scientific/ educational	Departments of education Scientific advisory bodies in many different fields	United Nations General Assembly (UNGA) UN Economic and Social Council (ECOSOC) UN Educational, Scientific and Cultural Organization (UNESCO) World Health Organization (WHO) International Labour Office (ILO) Food and Agriculture Organization of the United Nations (FAO) Intergovernmental Bureau for Informatics (IBI)
Economic/ trade policy	Departments of foreign affairs, trade, industry, commerce, etc Hardware/software producers	Organization for Economic Cooperation and Development (OECD) General Agreement on Tariffs and Trade (GATT) United Nations Centre on Transnational Corporations (UNCTC) International Chamber of Commerce
Protection of privacy	Departments of foreign affairs, justice Data Commissioners' offices Advisory bodies in many fields	Organization for Economic Cooperation and Development (OECD) Council of Europe (CoE) International Chamber of Commerce (ICC) Annual meetings of Data Commissioners
Developing country interests	Departments of foreign affairs Agencies for development aid Departments of trade/commerce Advisory bodies in different fields	United Nations General Assembly (UNGA) UN Economic and Social Council (ECOSOC) UN Centre on Transnational Corporations (UNCTC) United Nations Development Programme (UNDP) International Telecommunication Union (ITU) UN Educational, Scientific and Cultural Organization (UNESCO) Intergovernmental Bureau for Informatics (IBI) Organization for Economic Cooperation and Development (OECD)
Environmental problems	Departments of foreign affairs Departments of environment Scientific bodies in many fields	United Nations General Assembly (UNGA) UN Economic and Social Council (ECOSOC) UN Environment Programme (UNEP) UN Development Programme (UNDP) Organization for Economic Cooperation and Development (OECD)
Legal problems	Departments of foreign affairs, justice, commerce, transport, customs Statistical offices PTTs Patent offices Banks National trade facilitation bodies	United Nations Commission on International Trade Law (UNCITRAL) Organization for Economic Cooperation and Development (OECD) Council of Europe (CoE) International Civil Aviation Organization (ICAO) International Air Transport Association (IATA) International Union of Railways (UIC) International Rail Transport Committee (CIT) Central Office for International Railway Transport (OCTI) International Road Transport Union (IRU) Intergovernmental Maritime Consultative Organization (IMCO) International Chamber of Shipping (ICS) UN Economic Commission for Europe (ECE) Customs Cooperation Council (CCC) International Chamber of Commerce (ICC) Universal Postal Union (UPU) International Telecommunication Union (ITU) World Intellectual Property Organization (WIPO)
Trade data interchange	National trade facilitation bodies Departments of foreign affairs, transport Customs administrations Statistical offices National trade, transport, forwarding, insurance and payments organizations	UN Economic Commission for Europe (ECE) UN Conference on Trade and Development (UNCTAD) Customs Cooperation Council (CCC) International trade, transport, forwarding, insurance and payments organizations

CHAPTER 2.

Data Protection: Laws and National Policies

2.1 Data Protection Laws

2.1.1 Emergence of the Notion of "Data Privacy"

Although sensitive personal information constitutes something less than 10% of TDF*1, concerns over privacy protection gave rise to the first international discussions and legislation in this field.

In the 1960s, along with the spread of modern scientific and technical devices developed Western states began to be faced with the possible dangers of encroachment on human rights by the use of computers for processing personal information. Once personal data files are input into computer data bases in machine-readable form, together with the rapid global proliferation of computer facilities, the danger of the compilation and misuse of private information increased in part because of the difficulty of monitoring such processes.

Indeed, the legal concept of privacy has always been a rather confusing and somewhat complicated one. Nevertheless, an attempt has been made to define the concepts of privacy and data protection, which themselves are the successful result of an attempt to give a concrete form to the abstract notion of a

"right to be let alone"*2. In this context, the concept of privacy overlaps extensively with the concept of data protection. P. Sieghart of the United Kingdom's Data Protection Commission defines the term "privacy" as "the claim of the individual to decide for himself who shall know what about him, and what use they shall be entitled to make of that knowledge"*3. Explaining in more concrete manner, Professor Frosini, University of Rome, mentions the term "right to privacy" as follows:

> There no longer exists the freedom to refuse public information concerning personal data, but rather the freedom resides in the ability to control the use made of personal data inserted in a computer program. What now exists might be termed habeas data, and corresponds to the antique habeas corpus. Therefore, the right of access to data banks, the right to check their exactness, the right to bring them up-to-date and to correct them, the right to the secrecy of sensitive data, the right to authorise their dissemination: all these rights together today constitute the new right to privacy*4.

2.1.2 Fundamental Features of Data Protection Laws

Based on this new concept of privacy, since the beginning of the 1970s, several European states have passed data protection legislation making it compulsory for the public and private sectors to provide for the data subject whose data was collected, a form of "due process" supported by a series of regulatory mecnanisms to inspect, register and review data bases containing personal information. Although data protection legislation differs among states, they all contain certain basic provisions. These are

1. conditions on data processing in both the public and private sectors, including.
   - limitations on the kinds of personal data collected,
   - constant re-evaluation of the relevancy, accuracy, and completeness of the stored data,
   - specification of the purpose for which the data will be used;
   - guarantee of data security, in the form of technical and organizational safety measures.
2. the rights of data subjects with regard to the keepers or files, including·
   - the right to be informed that such data has been processed;
   - the right to have deleted or corrected

illegally processed or incorrect data,

- the right to safeguards against unauthorized access, including a right to compensation for damage caused by violations of privacy.

3. surveillance of data processing by a public data-protection agency*5

A further basic feature of data protection laws is "provisionality". It appears in the amendments which have been made frequently to data protection laws and in the so-called "sunset provisions" of these laws, in order to adapt to the rapid changes in technology and conditions surrounding TDF*6.

2.2 Different Legislative Approaches to Data Protection: 1973-1980

2.2.1 American "Bottom-Up" Approach and European "Top-Down" Approach

Despite all these common points, with the growth of international data communication networks, differences in national data protection laws have nevertheless arisen and become causes of potential international disputes. In particular, a noticeable difference in approach arose during the 1970s between the European laws governing privacy protection and those of the U.S.*7.

The approach taken by the U.S. in this period may be called the "bottom-up" approach, whereby the initiative for regulation of TDF is eschewed by government and entrusted to private data users. The fundamental feature of this approach, which draws heavily on the concepts of "freedom of speech" and the "freedom of the market", is that data users, free from governmental interference and armed with market information, choose appropriate standards of data protection, and in the due course of time companies providing standards not acceptable to the market will eventually die out in an evolutionary-like struggle for survival.

In contrast to this, European states, insisting on the supreme importance of the protection of personal privacy, decided that an international regulatory body of some form was needed to that end before any plan to allow the free flow of personal data could be adopted. However, until such a preventive structure is established, measures implementing data protection laws under the European civil law approach, as will be referred to later, must be taken by each respective nation. The approach taken by the European states during the 1970s may thus be expressed as the "top-down" approach, in other words, where the initiative is taken by public data-protection agencies*8.

These two approaches are also affected by a basic philosophical divergence between common law and civil law. Most European laws reflect the civil law tradition that it is

preferable to enact a law prior to the beginning of the situation which the law addresses. In addition, civil law tradition defines what is allowed instead of what is prohibited, forbidding anything that is not specified as permissible. In common law countries such as the U.S., on the other hand, law is usually formulated after problems occur, and anything not expressly forbidden is permitted*9.

As a result, the U.S. has enacted privacy protection laws on a sector-by-sector basis("sectoral approach")*10, while many European states have enacted data protection laws covering both public and private sectors ("omnibus approach")*11.

Two further significant differences which may be regarded as potential causes of international disputes will be considered in more detail in the next section.

2.2.2 Differences in Approach in TDF Legislation as Potential Causes of International Disputes

2.2.2.1 Differences in Provisions Regulating TDF

The first national European data protection law*12 was the Swedish Data Act of 1973*13.

In the elaboration of this Swedish Data Act, a part of general procedure of personal data protection to require the data user to obtain permission for automatic processing of

personal data. At that time, it was pointed out that Swedes' personal data could enter through international networks another state where such data are exposed to lower levels of protection ("data havens"), thereby potentially circumventing the operation of the Swedish Act. In order to avoid this danger, a further provision was passed whose sole object was to restrict the transfer abroad of Swedes' personal data. The section 11 of the 1973 Swedish Data Act provides as follows:

> If there is reason to believe that personal information will be used for A[utomatic] D[ata] P[rocessing] abroad the information may be issued only after permission by the Data Inspection Board. Such permission may be given only if there is ground to believe that the issuance will not cause undue encroachment on privacy...*14.

Under this section, between 1974 and 1983, the Data Inspection Board refused to grant a permission in the form of license for eight cases, which constituted 2.64% of all applications made concerning international data transfers, which totalled approximately 300 cases*15. When making its decision, the Board examines the nature of the personal information, the reason for collecting the data, the attitude of the data subject towards the transfer, and the purpose of the processing. An important factor for the decision of the

Board when granting a licence also seems to be the standard of data protection in the recipient's state*16. For example, the Board rejected the application of the Swedish subsidiary of Siemens, a German multinational corporation, for the transfer of data to the personal information system at its headquarters in Munich in 1974, because at that time West Germany had not yet adopted its data protection laws*17.

This section 11 of the Swedish Data Act became the model for similar provisions in other European data protection laws subsequently enacted in the 1970s*18.

2.2.2.2 Differences in provisions concerning "Legal Person" Privacy

Although these data protection laws focused primarily on the protection of privacy of individuals, during the 1970s, four European states, namely Austria, Denmark, Luxembourg and Norway*19, brought "legal persons" within the scope of their data protection laws. This means that corporations and other organizations or associations falling under this definition would receive similar privacy protection as would individuals*20. The major justification for the extension of laws' application to legal person was that in these four countries, small enterprises played an important economic role. Thus if an individual carried on a business as a sole

proprietor, then his/her personal information, e.g. credit information, was accessible in a company's files*21. Because an individual should not lose his/her right to privacy by simple reason of acting as a one-man business, it was necessary to formulate a flexible legal framework to protect the sole proprietor's privacy.

It was reported that while corporations in these four countries generally accepted their legislations, they also assumed that "strategic company files [would] be exempt from the law on a case-by-case basis through arrangements with the [national] data authorities"*22. If such files were not excluded, the legislation would then enable a company to access data regarding itself held by its competitor, under the pretext of exercising its right to privacy protection, i.e. checking the accuracy of such information. This exercise of the company's right would constitute a legalised form of "industrial espionage", allowing the company to gain a potential competitive advantage*23.

2.3 Need for International Adjustment of Conflicting National Policies

By including "legal person" as a data subject in national data protection laws under the pretext of "privacy protection", trade secrets in the form of "bussiness (corporation) data"

would be protected, but without any proper international standards. Moreover, with the combination of provisions concerning TDF regulation and those concerning "legal person" privacy protection, it can be seen that the data protection laws are used for objectives other than those specified in the laws themselves, for example, as non-tariff barriers to the international trade in services

Therefore, at the end of the 1970s, the U.S., whose federal privacy protection laws provided measures concerning neither TDF regulation nor "legal person" privacy, began to denounce the existence of these two provisions as unfair trade barriers*24. This viewpoint of the U.S. has a concrete form in law. For example, Section 305(a)(1) of the 1984 Trade and Tariff Act *25 amends Section 301 of the 1974 Trade Act*26 to seek to obtain maximum freedom for international trade and investment in high technology products and related services. It clearly defines, but does not limit, the following as barriers to the export of U.S. services

> [Under the grouping of] restrictions on the operation of enterprises in foreign markets. [...]
>
> - direct or indirect restrictions on the transfer of information into, or out of, the country or instrumentality concerned, and

- restrictions on the use of data-processing facilities within or outside of such country or instrumentality*27.

Furthermore, because the U.S. courts can request the parties to a cail to produce documents located outside the U.S., even if doing so would violate foreign data protection laws which prohibite tneir disclosure, such extraterritorial application of U.S. jurisdiction may give rise to the problems of choice of jurisdiction, choice ot applicable law and recognition of foreign judgments*28.

Consequently, these differences in approach in domestic data protection laws became a potential cause of international conflict as well as the fears that possible violations of personal privacy protection might occur through TDF, and the fears that an international regulation of transborder flows of personal data might be used for other restrictive purposes. As a result, the two organizations mentioned above, namely the OECD and the CoE, set about to harmonize national laws which reflected conflicting national policies regarding TDF.

Footnotes to CHAPTER 2

*1 T.M. Rankin, "Business Secrets across International Borders: One aspect of the Transborder Data Flow debate" (March/April 1986) Computer L. & Prac. 106 at 108.

*2 S. Warren & L. Brandeis. "The Right to Privacy" (1890) 4 Harv. L. Rev. 193.

*3 P. Sieghart, "The Protection of Personal Data -- Lacuna and Overlap" in OECD, Transborder Data Flows and the Protection of Privacy, OECD/ICCP Series No.1, (Paris: OECD, 1979) at 226.

*4 V. Frosini, "The European Convention on Data Protection" (January/February 1987) 84 at 85. See also A.W. Branscomb, "Who Owns Information?" (January 1986) 9 T.D.R. 9.

*5 See R. Ellger, "European Data Protection Laws as Non-Tariff Barriers to the Transborder Flows of Information" in Mestmacker, supra, CHAPTER 1 note 11 at 123. See also, The OECD Guidelines, supra, INTRODUCTION note 4 at 10-11 [Part two: Basic Principles of National Application].

*6 H. Burkert, "International Data Protection" (May/June 1985) Computer L. & Prac. 155 at 156. For example, Swedish data protection law were amended five times from July 1973 of enforcement to April 1988.

*7 In fact, the manifold differences of various data protection laws seem to constitute the new field of comparative legal study. However, for the purpose of this thesis, the differences between the European laws and the U. S. laws will be mainly treated. For a general comparative study of data protection laws, see F. Hondius, "Data Law in Europe" (1980) 16 Stan. J. Int'l L. 87 at 93-102; J.H. Yurow, "Data Protection" in A.W. Branscomb, ed., Toward a Law of Global Communications Networks (New York: Longman, 1986) at 240-244.

*8 See M. Briat, "Personal Data and the Free Flow of

Information" in P. Hansen et al., Freedom of Data Flows and EEC Law [Proceedings of 2nd CELIM Conference] (Deventer, Netherlands: Kluwer, 1988) at 48; Yurow, supra, note 7 at 243-244.

*9 See E.W. Ploman, "Transborder Data Flows The international legal framework" (Spring 1982) 3 Computer/L. J. 551 at 552-553, Hondius, supra, note 7 at 97-98.

*10 The primary U.S. initiative was the Privacy Act of 1974 [5 U.S.C. s. 552 (a)]. Other U.S. sectoral legislation includes Family Educational Rights and Privacy Act of 1974 [20 U.S.C. s. 1232 (g), as amended by Pub. L. No.96-26, 93 Stat. 342], Fair Credit Reporting Act [15 U.S.C. s. 1681, et. seq.], Right to Financial Privacy Act of 1978 [12 U.S.C. s. 3401, et. seq.], Tax Reform Act of 1976 [26 U.S.C. s. 7609]. For a detailed survey concerning sectoral approach of the U.S federal privacy protection laws, see J.H. Yurow, ed. Issues in International Telecommunications Policy: A sourcebook (Washington, D.C. Center For Telecommunications Studies, The George Washington University, 1983) at 148-153.

*11 For a summary of omnibus European data protection laws, see Yurow, supra, note 10 at 154-162.

*12 The first data protection statute of all was the Hessian Data Protection Act of 7 October 1970 [1970 Hess. Gesetz und Verordnungsblatt (GVBI.) I 625]. The application of this law is limited to the German state of Hessen.

*13 Datalag, 1973 SFS 289.

*14 G.S. Grossman, "Transborder Data Flow Separating the privacy interests of individuals and corporations" (1982) 4 Nw. J. Int'l L. & Bus. 1 at 23 note 66.

*15 Ellger, supra, note 5 at 129.

*16 Ibid.

*17 Ibid. (Decision of March 13, 1975 (Siemens case),

No.3103-74). Later Siemens decided to apply the FDR's Federal Data Protection Act of 1977 to their company ["FDR: Siemens makes protection routine" (November 1986) 9 T.D.R. 22].

*18 See Article 32 of the Austrian Personal Data Protection Act [Bundesgesetz vom 18. Oktober 1978 uber den Schutz personenbezogener Daten, 1978 Bundesgesetzblatt (BGBI.) 3619];
Article 21 of the Danish Act on Private Registers [Lov om private registre m. v., Lov nr.293 af 8. juni 1978, 1978 Lovtidend A 833];
Article 24 of the French Act on Informatics, Files and Freedom [Loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 1978 J. O. 227];
Article 24 and 32 of the German Act for the Protection Against the Misuse of Personal Data [Gasetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. Januar 1977, 1977 BGBI. 1201];
Article 3 of the Luxemburg Act Regulating the Use of Personal Data in Data Processing [Loi du 31 mars 1979, réglementant l'ultilisation des données nominatives dans les traitements informatiques, 29 Mémorial A 582, 11 avril 1979];
Article 36 of the Norwegian Act on Personal Registers [Lov om personregistre m. m. av 9. juni 1978, no.48, 1978 Norsk Lovtidende 402].

For English translations, see Yurow, supra, note 10 at 154-160.

*19 See: Article 3.2 of the Austrian Personal Data Protection Act [supra, note 18];
Article 1 of the Danish Act on Private Registers [supra, note 18],
Article 2 of the Luxemburg Act Regulating the Use of Personal Data in Data Processing [supra, note 18];
Article 1 of the Norwegian Act on Personal Registers [supra,

note 18].

*20 There is certain support for this inclusion of legal persons in article 25 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [4 November 1950, 213 U.N.T.S. 221], which allows non-governmental organizations to allege violations of human rights against the government, including the right to privacy [art. 8(1)].

*21 See "Denmark: Legal Person Coverage" (January 1986) 9 T.D.R. 30.

*22 Yurow, supra, note 7 at 246.

*23 I.N. Walden & R.N. Savage, "Data Protection and Privacy Laws: Should organizations be protected?" (1988) 37 Int'l & Comp. L. Q. 337 at 345.

*24 See J.M. Eger, "Emerging Restrictions on Transborder Data Flows: Privacy protection or non-tariff trade barriers?" (1978) 10 L. & Pol'y Int'l Bus. 1055 at 1055-1060; P.E. Cole, "New Challenges to the U.S. Multinational Corporation in the European Economic Community: Data protection laws" (1985) 17 Int'l L. & Pol. 893 at 916-917.

*25 1984 Trade and Tariff Act [Pub. L. No.98-573]

*26 1974 Trade Act [Pub. L. No.93-618]

*27 Section 305(a)(1) of the 1984 Trade and Tariff Act [supra, note 25, 98 Stat. 3006] at 3008. See also, U.S. Congress, Senate, Committee on Commerce, Science and Transportation, Long Range Goals in International Telecommunications and Information: An Outline for United State Policy [Report of the National Telecommunications and Information Administration, Committee Print 98-22, 98th Cong., 1st Sess., March 11, 1983] (Washington, D.C,: U.S. Government Printing Office) at XI-XV and 5-34.

*28 See United States v. Bank of Nova Scotia (691 F.2d 1384 (11th Cir. 1982)), United States v. Bank of Nova Scotia (740

F.2d 817 (11th Cir. 1984), cert. denied, 105 S.Ct. 778 (1985)). See also, J.T. Burnett, "Information, Banking Law and Extraterritoriality" (January 1986) 9 T.D.R. 17 at 17-18; P. Robinson, "Legal Issues Raised by Transborder Data Flow" 11 Canada - United States Law Journal 295 at 305-309 (1986).

CHAPTER 3.

Harmonizing Data Protection Laws.

Measures Taken by the OECD and the Council of Europe(CoE)

3.1 Comparative Analysis of the OECD Guidelines and the CoE Convention

3.1.1 Preliminary Steps of the OECD and the CoE

3.1.1.1 The OECD

The OECD program for TDF originated from computer utilisation studies in the public sector which began in 1969*1. Specific concern by various parties about TDF, following the introduction of data protection laws, arose from 1970. In 1971, a consultant's report was received on digital information and the privacy problem*2. In 1974, the OECD seminar on Policy Issues in Data Protection and Privacy considered the problems that might arise from the enforcement of domestic data protection laws on TDF*3. Between 1974 and 1977, the OECD Data Bank Panel analyzed and studied the privacy issues, seeking to identify basic rules of data protection and data security. The Panel organized a symposium in Vienna in 1977. Following this symposium, it was perceived that the problem of the protection of personal data might require a more effective organizational

framework within the OECD. As a result, the existing two subordinate organs under the Committee for Scientific and Technological Policy, i.e. the Information Policy Group (set up in 1965) and the Computer Utilisation Group (set up in 1969) were merged in 1977 into the Working Party on Information, Computer and Communication Policy (ICCP). The mandate of this Working Party on ICCP was a wide one which encompassed scientific, technical, economic, social, cultural and legal impacts of information, computer and communications systems, since the integrated approach of these matters was regarded necessary to tackle the national and international aspects of this rapidly expanding area which had important economic and social consequences for member countries' economies*4. Later in April 1982, taking account of the importance of its mandate, the Working Party on ICCP was raised to the Committee on Information, Computer and Communication Policy. As a part of the major projects of this Working Party on ICCP, an ad hoc inter-governmental Group of Experts on Transborder Data Barriers and the Protection of Privacy was formally established in 1978. The terms of reference of the Group of Experts were

1. To develop guidelines on basic rules governing transborder flow and the protection of personal data and privacy in order to facilitate a harmonization of national legislation, without precluding

the establishment of an international convention at a later date;

2. To investigate the legal and economic problems relating to the transborder flow of non-personal data in order to provide a basis for the development of guidelines in this area to take into account the principle of free flow of information*5.

The Group of Experts was instructed to carry out its activities in close co-operation and consultation with the CoE and the EC, and to complete its work on the first term of reference by 1 July 1979. On 21 November 1979, the Group of Experts presented draft Guidelines and an Explanatory Memorandum to the Committee for Scientific and Technological Policy of the OECD*6. Finally, the Council Recommendation with the OECD Guidelines was adopted and became applicable on 23 September 1980.

3.1.1.2 The CoE

In 1968, the CoE's Parliamentary Assembly (later Consultative Assembly) recommended the CoE's Committee of Ministers to study the possible dangers of encroachment on human rights posed by the use of modern scientific and technical devices*7. In 1970, the Committee of Experts on Data Protection reported to the Committee of Ministers that, whereas

routine civil and criminal legislation could efficiently check abuses of technical devices, the use of computers for processing personal information raised new and fundamentally different questions requiring novel solutions. The Committee of Experts also reported that the mechanisms and remedies offered by the European Human Rights Convention*8 provided inadequate solutions to such computer-related problems*9.

On the basis of the conclusions of the Committee of Experts, the Committee of Ministers directed an inter-governmental committee to draw up new legal rules on data protection. These rules appeared in two Resolutions of the Committee of Ministers recommending that governments of member states give effect in their domestic law to a number of basic principles to protect "the privacy of individuals (physical persons) vis-à-vis electronic data banks*10." In the view of the conformity of member countries' domestic data protection laws, however, it seemed desirable to convert the non-binding recommendations set out in these two resolutions into binding provisions, i.e. in the form of a convention. Thus, in 1976, the CoE directed the Committee of Experts to draw up an international treaty, working in close co-operation with the OECD. In May 1979, the Committee of Experts finalized a draft treaty*11 and circulated it to the governments of the member states for comment. Finally, the CoE Convention was adopted in 17 September 1980 and opened for signature by member states on

28 January 1981.

3.1.2 Stance Taken by the OECD and the CoE towards these Guidelines and Convention

Concern about the social implications of computer development was expressed by both the OECD and the CoE as early as the end of the 1960s. However, the two organizations emphasized different considerations when they began to tackle the growing international aspects of TDF issues.

3.1.2.1 The OECD

The aims of the OECD are to promote policies designed

1. To achieve the highest sustainable economic growth and employment and a rising standard of living in member countries, while maintaining financial stability, and thus to contribute to the development of the world economy.. ;
2. To contribute to sound economic expansion in member as well as non-member countries in the process of economic development;
3. To contribute to the expansion of world trade on a multilateral, non-discriminatory basis, in

accordance with international obligations*12.

Under these aims of the organization, all the activities relating to TDF undertaken by the OECD are intended to control the influence of telematics on the economies of its member states. Moreover, while recognising that its member states "have a common interest in protecting privacy and individual liberties*13" the OECD strives to ensure the free flow of information and to avoid obstacles to international trade. Furthermore, as seen in the second paragraph of its mandate, the Group of Experts on Transborder Data Barriers and the Protection of Privacy has dealt with transborder flows of non-personal data, anticipating "protectionist challenges before they become urgent*14" since the year following its establishment in 1978.

3.1.2.2 The CoE

The CoE, which consisted of seventeen European states in 1968 when it first began extensive consideration of the question concerning the connection between technology and human rights, has now expanded to include twenty-two members, as of April 1990. Its purpose is the promotion of greater European unity, with special emphasis on the rule of law and human rights. The member states cooperate to this end both at

inter-governmental and inter-parliamentary levels*15. Because The CoE's activities on TDF derived from the study regarding the question of adequate protection of the individual's right of privacy vis-à-vis modern science and technology, the primary objective of its activities concerning TDF is on the influence of telematics on human rights. Its activities thus deal exclusively with personal data.

3.1.3 Special Features of the Rules

There is in fact no great difference between the composition and contents of the OECD Guidelines and the CoE Convention. Both instruments recognize the existence of two basic but competing values in the field of personal data protection, i.e. the protection of privacy and individual liberties and the advancement of the transborder flows of personal data. As a means of reconciling these principles, both instruments establish a set of fundamental principles for the protection of privacy at both the national and international levels, and provide mechanisms for mutual assistance and consultation to ensure the observance of their closely-resembling rules*16. The reason for this result was brought about by the fact that, during the dratting of the two instruments, both working groups, i.e. the Group of Experts of the OECD and the Committee of Experts of the CoE maintained

This fact, consequently, makes the coincidence of the adoptions between the OECD Guidelines and the CoE Convention all the more significant. As it is presumed that, any differences observed between the two instruments may indicate the points in dispute that European states of the CoE and non-European states of the OECD, above all the U.S., could not reach accord on, by the time of the adoptions of the two instruments.

3.1.3.1 The Legal Nature of the Rules

The most important difference between the two instruments, and thus between the respective rules contained in them, is that the CoE Convention is a "contractual commitment" and is legally binding the contracting states, whereas the OECD Guidelines constitute an "advice", and therefore have no such power to bind member states*18.

Actually, in close co-operation for drafting data protection instruments, it had been explored whether the CoE and the OECD could jointly sponsor the convocation of a diplomatic conference for the conclusion of an international convention. This project was abandoned, however, when it became clear that the largest OECD member, the U.S. was not in favour of a binding instrument, partly because of the fear of some American multinational corporations "that the continuity

or confidentiality of existing international non[-]personal data flows might be interrupted*19". This may be the reason why the OECD Guidelines show a tendency to emphasize and support voluntary self-regulation of private data users, whether in the form of codes of conduct or otherwise, in observing the basic principle of the protection of privacy and personal data [paras. 3(a), 18, and 19].

In the meantime, the CoE Convention, to which the U.S. is not a party, requires signing states to enact new or modify existing data protection laws [art. 4] to meet its specifications guided by the principle of reciprocity [arts. 3(4) and (5)], and further to designate national authorities to secure the domestic implementation of its rules, especially those concerning foreign residents in their pursuit of their privacy rights [arts. 14 to 17]. Moreover, no reservations are allowed to the CoE Convention [art. 25]. While the OECD Guidelines refer to these same points for the protection of personal data, but in the form of non-binding recommendation [the Recommendation paras.1 and 3; the Guidelines paras. 15, 19, and 21].

3.1.3.2 Rules Regulating TDF

Article 12 (2) of the CoE Convention states that a party shall not·

> [F]or the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flow of personal data going to the territory of another Party.

But it also provides two exemptions in the following two cases:

1. Where its legislation includes specific regulations for certain categories of data and the regulations of the recipient state don't provide equal protection [art. 12(3)(a)],
2. Where the transfer is intended to reach the territory of a non-contracting state through the intermediary of the territory of another contracting state, in order to obtain the advantages from the usage of "data havens" [art. 12(3)(b)].

Under these exemption clauses, it is possible that where one party, having extended the application of the CoE Convention to legal persons [art. 3(2)(b)], may legitimately refuse the transfer of data to recipient states which have not yet enacted a similar extension, by claiming that the protection level of those states is not equivalent to its own. Even where those recipient states have otherwise complied with the principles of the CoE Convention, under article 3 (5), they are not allowed to claim the application of the CoE Convention

on this point.

As regards these two exemptions to the rule of free TDF, paragraph 17 of the OECD Guidelines indicates the same points, closely corresponding to paragraphs 15 and 16.

However, as mentioned above, the OECD Guidelines emphasize more strongly and repeatedly the importance of free flow of information, thus the Council of the OECD recognized in the Preamble of the Recommendation of 23 September 1980.

> [T]hat, although national laws and policies may differ, Member countries have a common interest ... in reconciling fundamental but competing values such as privacy and the free flow of information,
>
> 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.

Then, paragraph 2 of the Recommendation suggests:

> That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified

obstacles to transborder flows of personal data.

Furthermore, paragraph 18 of the OECD Guidelines suggests that states should avoid:

> [D]eveloping 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.

Therefore, it may be assumed, as D. Cooper observes, that the real intention of the statement of paragraphs 15, 16 and 17 of the OECD Guidelines is to provide the "quid pro quo" which the member countries, especially the U.S., receive in return for adapting domestic laws to meet the demands of their data-trading partners, i.e. European countries, in order to secure their support for the OECD Guidelines*20.

3.1.3.3 Rules concerning "Legal Person" Privacy

Regarding the data subjects, the OECD Guidelines confined their definition to individuals, and left to member states the tasks of drawing the dividing line between personal and non-personal data and of deciding policies with regard to the

"'legal person' privacy" issue. The OECD explains the reason for this decision as follows:

> [T]he 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.*21

However, it was reported that some members of the Group of Experts advocated "that the possibility of extending [the OECD Guidelines] to legal persons (corporations, associations) should be provided for." This suggestion, though, did not secure sufficient support*22.

On the other hand, although legal persons are not included in the main body of the CoE Convention, article 3 (2) (b) prescribes that national data protection laws can be extended to information relating to

> [G]roups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.

It continues by saying that states which include such categories in their data protection legislation may then invoke the rule of reciprocity with regard to states who have not made such extensions [art. 3(4)].

3.1.4 Implementation Procedure of the Rules

3.1.4.1 The OECD

As regards the national implementation of the principles enumerated in Parts Two and Three, the OECD Guidelines advises, in Part Four, that member states should "establish legal, administrative or other procedures or institutions" [para. 19]. These measures include the adoption of appropriate domestic legislation [para. 19(a)]; encouragement and support for self-regulation, in the form of codes of conduct or otherwise [para. 19(b)], which is addressed "primarily to common law countries where non-legislative implementation of [the OECD Guidelines] would complement legislative action*23."

The OECD Council Recommendation of 23 September 1980 [the Recommendation paras. 3 and 4] and the OECD Guidelines [paras. 20 and 21] also mention without going into detail, the necessity of mutual assistance and specific procedures for consultation and co-operation for the application of the OECD

Guidelines. For those purposes, an ad hoc group has met since 1981 nearly biennially, with attendance by almost all member countries. The ad hoc meetings for the follow-up of the OECD Guidelines have been held to date on four occasions. 5-6 October 1981, 10-11 March 1983; 25-26 June 1985, and, 10-11 May 1988. For every ad hoc meeting, the OECD Secretariat/ICCP Division*24, using the results of questionnaires completed and returned by member states, prepares the synthesis report on the application of the OECD Guidelines which is distributed to the representatives of member states at the meeting. The questionnaires have sought, from the first meeting of 1981, essentially the following information:

1. Are comprehensive national data protection laws currently in force and, if so, what is their form and scope? In particular, do they contain the principles of the OECD Guidelines?,
2. If no data protection laws exist then what proposals, if any, exist in the area and what is the likely time frame for the adoption of any such proposals?,
3. The general experience of member countries with data protection laws,
4. The ongoing role and relevance of the OECD Guidelines and comments on the likely future direction to be taken in this area*25.

With every survey conducted by the OECD Secretariat,

almost all member countries have responded to the questionnaire and many of them provide material in addition to that sought by the questionnaire*26. It is thus reasonable to predict that, by these follow-up meetings, the member states will obtain both an excellent indication of the overall legislative trends, and other information gained from other members' experiences in the field of TDF.

Although the institutional framework is dealt without going into detail, under the OECD Guidelines, as will be referred to later, the follow-up mechanism aims to keep the rules for personal data protection adaptable to changing environments and emerging problems, by means of exchanging experiences gained in member states from their data protection legislation and concrete problems of a national and international nature.

3.1.4.2 The CoE

For the CoE Convention, the key machinery for implementation is the data protection legislation of the contracting states since the enactment of national legislation standardizing the principles of Chapters II and III is a condition for ratifying the CoE Convention [art. 4].

Based on this condition, Chapters IV and V of the CoE Convention provide for mutual assistance and consultation among

the Parties. Chapter IV treats mutual assistance in order to implement the CoE Convention and to assist data subjects resident abroad in exercising the rights conferred by their domestic laws. Further, Chapter V provides for the establishment of a Consultative Committee. Article 19 prescribes the functions of the Consultative Committee as follows:

1. To make proposals with a view to facilitating or improving the application of the CoE Convention,
2. To make proposals for amendment of the CoE Convention in accordance with article 21,
3. To formulate its opinion on any proposal for amendment of the CoE Convention which is referred to it in accordance with article 21 (3),
4. To express, at the request of a contracting state, an opinion on any question concerning the application of the CoE Convention.

In accordance with articles 18 and 20, the Consultative Committee was set up in June 1986, after the entry into force of the CoE Convention, by the representatives of all five contracting countries which ratified the CoE Convention, namely France, the FRG, Norway, Spain and Sweden, although ten non-contracting countries which signed the CoE Convention also sent observers. This first meeting was spent discussing its rules of procedure, e.g. working methods, voting, the role of

the chairman and admission of observers*27.

As of April 1990, the Consultative Committee has met on three occasions. At its third meeting in May 1989, the representatives of eight ratifying countries, namely, the above five countries plus Austria, Luxembourg, the UK, gathered and dealt with, above all, the issue of "equivalent protection" in the context of TDF*28.

3.1.5 Present State of the Member Countries' Domestic Legislation

The CoE Convention was adopted by all the participants, although not all of them signed it immediately. It might have been easier for the CoE member states to conclude a legally-binding accord, because, compared to OECD members, a greater proportion of them already had established national data protection laws that provided an existing basis on which they could narrow the scope and set up standards agreeable on data protection principles. After the entry into force of the CoE Convention in October 1985, the Committee of Ministers of the CoE may invite any country not a member of the CoE to accede to the CoE Convention [art. 23]. However, as of April 1990, any non-member country of the CoE, including the U.S. which dominates the international computer and telecommunications markets, did not sign the CoE Convention.

Thus, at this time, ten of the twenty-two CoE countries have ratified the CoE Convention, and a further eight members have signed but not as yet ratified it*29.

As regards the OECD Guidelines, they were not adopted unanimously. When they were adopted in September 1980, eighteen of the twenty-four OECD member countries voted for the proposal, while six countries, namely Australia, Canada, Iceland, Ireland, Turkey and the U.K. abstained, either for substantive reasons or because their governments had yet to establish national data protection policies*30. However, by the time of May 1988 when the fourth ad hoc meeting on the follow-up of the OECD Guidelines was held, all member states had subscribed to the OECD Guidelines*31.

In 1980 when the two instruments were adopted, nine countries had national data protection legislation. However the number of countries with data protection laws gradually increased. As of April 1990, eighteen of the twenty-four OECD member countries have national data protection laws and thirteen of those eighteen countries have overlapping membership with the CoE*32.

3.2 Limitations of a Comparative Examination of the Effectiveness of these Measures

As mentioned above, the legal nature of the OECD

Guidelines is a recommendation of an international organization, and does not legally bind its member states*33. On the other hand, the CoE Convention is an accord which binds its member states. Moreover, it is not a "self-executing" treaty. Thus, after ratifying the CoE Convention, states have to make the necessary changes to their domestic laws to give effect to the fundamental principles of data protection set out in it (art. 4).

However, it is not easy to estimate the degree or effectiveness or either instrument simply by looking at the differences in their structure and provisions, and above all difference in their respective legal nature.

Firstly, it may not be reasonable if we do not approve any effectiveness or the CoE Convention during the period from 28 January 1981, the date when it was opened for signature, to 1 October 1985, the date when it entered into force. One example of this statement is the UK Data Protection Act of 1984*34. It is reported that one of the major objectives of this legislation was to avoid restrictions on the transfer of data for storage and processing in the UK, if in case the U.K. had not yet adopted its data protection laws whose standards of data protection met with the requirements of the CoE Convention*35.

Secondly, nor can a straightforward comparison be made of the follow-up activities by the two bodies, for the simple

reason that, whereas the Consultative Committee of the CoE Convention came into substantitive operation only in May 1988, the OECD had already held four ad hoc follow-up meetings under the OECD Guidelines by then, and the Consultative Committee of the CoE Convention had not yet generated enough material to allow adequate analysis.

Thirdly, it may be impossible to determine by just how much the application of the two instruments has been affected by political and economic factors, as already observed in competing national policies in the field of TDF.

Despite these limitations, it can not be denied that, as will be examined later, the OECD Guidelines do ultimately function as a means of making the member states (and other players in the field of TDF, e.g. multinational enterprises) behave in certain controlled manner, namely in a manner expected in their "not-enforceable" rules.

Taking into account these limitations, the next chapter will confirm the influence of the two instruments on the national data protection policies of the member states.

Footnote to CHAPTER 3

*1 The OECD Guidelines, supra, INTRODUCTION note 4 at 19 (para. 16).

*2 See G. Niblett, Digital Information and the Privacy Problem, OECD Informatics Studies No.2, (Paris OECD, 1971).

*3 See OECD, Policy Issues in Data Protection and Privacy, OECD Informatics Studies No.10, (Paris: OECD, 1976).

*4 For detailed information concerning the major projects of the Working Party on ICCP, see D. Kimbel, "Policy Research for Information Activities: The OECD Programme on Information, Computers and Communications Policy" (December 1977) Telecom. Pol'y 367.

*5 OECD Doc. DSTI/ICCP/78.6 [mandate of the Group of Experts], cited from: M D. Kirby "Transborder Data Flows and the 'Basic Rules' of Data Privacy" (1980) 16 Stan. J. Int'l L. 27 at 43 note 49.

*6 OECD, "Draft Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (1980) 19 I.L.M. 318.

*7 Consultative Assembly of the Council of Europe, Rec.509 (1968), (1967-68) Official Report: Session 19 at 763.

*8 Supra, CHAPTER 2 note 20.

*9 Hondius, supra, CHAPTER 2 note 7 at 91-92.

*10 Council of Europe, Committee of Ministers Resolution (73)22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector (adopted 26 September 1973), and Resolution (74)29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (adopted 20 September 1974), as described in: Council of Europe, (1983) 14 Information Bulletin on Legal Activities within the Council of Europe and in member states 15.

*11 Council of Europe, "The draft Convention for the Protection of Individuals with regard to Automatic Processing of Persoanl Data of the Council of Europe" (1980) 19 I.L.M. 284.

*12 Convention of the Organization for Economic Co-operation and Development, 14 December 1960, 21 U.K.T.S. Cmnd. 1646 [hereinafter Convention of the OECD], art. 1.

*13 The OECD Guidelines, supra, INTRODUCTION note 4 at 7 [Preamble].

*14 "OECD Data Flow Pledge Planned" (1982) 5 T.D.R. 3.

*15 A.H. Robertson, The Council of Europe Its structure, functions and achievements (London. Stevens, 1961) at 10-15. See also, Statute of the Council of Europe, 5 May 1949, 87 U.N.T.S. 103, art. 1.

*16 Both the Guidelines [Part Two] and the Convention [Chapter II] provide so-called "basic principles of national application" as minimum standards which should be implemented by both member states. They are enumerated as follows

1. Collection Limitation Principle [para. 7 / art. 5 (a)];
2. Data Quality Principle [para. 8 / arts. 5 (c) and (d) (limited to automatically processed personal data)],
3. Purpose Specification Principle [para. 9 / art 5 (c) (partially to the terms "legitimate purposes")],
4. Use Limitation Principle [para. 10 / art. 5 (c) (partially from the terms "not used")],
5. Security Safeguards Principle [para. 11 / art. 7],
6. Openness Principle [para. 12 / art. 8 (a) (as "additional safeguards")],
7. Individual Participation Principle [para. 13 / arts. 8 (b), (c) and (d)],
8. Accountability Principle [para. 14 / art. 13],

9 Time Limitation Principle[(not specified in the Guidelines / art. 5 (e)].

The name of the Principles except the principle 9, follows the usage of the OECD Guidelines. The name "Time Limitation Principle" is as used in Kirby, supra, note 5 at 64.

For a comparative survey of the rules of the OECD Guidelines and the CoE Convention, see Kirby, supra, note 5, P H Patrick, "Privacy Restrictions on Transnational Data Flows A comparison of the Council of Europe Draft Convention and OECD Guidelines" (1981) 22 Jurimetrics Journal 405; W.J. Kirsch, "The Protection of Privacy and Transborder Flows of Personal Data The work of the Council of Europe, the Organization for Economic Co-operation and Development and the European Economic Community" (1982) 21 Legal Issues of European Integration 21· and J.A. Zimmerman "Transborder Data Flows; Problems with the Council of Europe convention, or protecting states from protectionism" (1982) 4 Nw. J. Int'l L. & Bus. 601.

*17 The OECD Guidelines supra, INTRODUCTION note 4 at 21 (para. 20).

*18 Patrick, supra, note 16 at 407.

*19 A.O. Roth, "Introductory Note" 19 I.L.M. (1980) 282 at 283. See also, F. Hondius, "A Decade of International Data Protection" (1983) 30 Netherlands Int'l L. Rev. 103 at 113.

*20 D.M. Cooper, "Transborder Data Flow and the Protection of Privacy The harmonization of data protection law" (Summer 1984) The Flecher Forum 335 at 345.

*21 The OECD Guidelines, supra, INTRODUCTION note 4 at 24 (para. 33).

*22 Ibid.

*23 The OECD Guidelines, supra, INTRODUCTION note 4 at 34 (para. 70).

*24 The ICCP Division is the Secretariat supporting the

Working Party on ICCP by preparing meetings and conferences, documents, reports and publications. See OECD, Policy Issues in Data Protection and Privacy, OECD/ICCP Series No.4, (Paris OECD, 1980) at 162.

*25 A copy of the questionnaire for the second ad hoc meeting of 1983 [OECD Doc. DSTI/ICCP/83.17] is contained in ANNEX 3 of this thesis, which was public released at the Second OECD Symposium on TDF in London, 30 November - 2 December 1983.

*26 The synthesis report of second ad hoc meeting on the follow-up of the OECD Guidelines was revised and reprinted in M. Briat, "Synthesis Report on the Application of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data -- Update as of December 1983" in OECD, ed., Transborder Data Flows -- Proceedings of an OECD Conference (Amsterdam. North-Holland, 1985) at 351-391. A summary of this report which was produced by Transnational Data Reporting Service is contained in ANNEX 3 of this thesis [reproduced from (January/February 1984) 7 T.D.R. 4].

*27 Council of Europe, (1987) 24 Information Bulletin on Legal Activities within the Council of Europe and in memeber states 23-24.

*28 "Council of Europe Consultative Committee Meets" (August/September 1989) 12 T.D.R. 28.

*29 See ANNEX 4 of this thesis [Status of Data Protection Legislation - April 1990].

*30 Patrick, supra, note 16 at 407.

*31 In order to make the OECD operations more flexible, article 6(2) of Convention of the OECD [supra, note 12], provides that a member country may abstain from voting. In such a case, the abstention does not preclude the adoption of the decision or a recommendation, which becomes applicable to the other member countries. For example, six member countries

which abstained from voting for the adoption of the OECD Recommendations concerning the OECD Guidelines of 23 September 1980, later adopted them respectively as follows: Australia, 10 December 1984, Canada, 29 June 1984; Iceland, 28 October 1980; Ireland, 12 June 1986, Turkey 21 January 1981, the U.K., 23 September 1981. The information regarding the date of adoption of the OECD Guidelines was provided during an interview in June 1988 with Mr. Muramatsu, Director for International Planning and Research, Management and Co ordination Agency (MCA), Government of Japan, who in turn obtained the information from the OECD document [DSTI/ICCP/88.5], because public release of the documents concerning ad hoc follow-up meetings was in principle restricted.

*32 See ANNEX 4 of this thesis [Status of Data Protection Legislation - April 1990].

*33 Convention of the OECD, supra, note 12, art. 5(b).

*34 Data Protection Act 1984 (U.K.), 1984, c.35.

*35 Robinson, supra, CHAPTER 1 note 10 at 17

CHAPTER 4.

Evaluation of the Achievement of

the OECD and the CoE 1980-1990

4.1 Adoption of the "Bottom-Up" Approach

4.1.1 The Simplification of Data Protection Procedures

Regarding the adoption of the "bottom-up" approach, this approach in existing data protection legislation can be observed in the simplification of data protection procedures in " top-down" approach for reducing the administrative burden. As a result of the practices surrounding applications under licensing or registration systems in the early 1970s, the European countries with this type of system have gradually come to realize that in receiving and processing the application of data users, it gave rise to a large and costly administration. Accordingly, they have decided to shift their legislative emphasis from a strict authorisation or licensing system towards one of notification or registration, and even the existing notification/registration system has been amended to adopt a streamlined approach which requires only certain "sensitive" categories of personal data to be registered. Thus, the seven European OECD members*1 which had enacted data protection legislation by 1987, responding to a questionnaire

sent to OECD members for the preparation of the fourth ad hoc meeting on the follow-up of the OECD Guidelines, stated that they had adopted a simplified procedure of notification/registration in order to encourage full and complete applications by the relevant users.

4.1.2 Voluntary Corporate Compliance with the Data Protection Principles of the OECD Guidelines and the CoE Convention

Before the adoption of the OECD Guidelines and the CoE Convention, the leading measure for protecting personal data was the imposition of data protection legislation by public data protection agencies as a "top-down" approach. However, after 1980 and especially over recent years, there has been seen the genesis of a "bottom-up" approach. Under this approach, systems of self-regulation concerning the protection of personal data have been set up in particular in countries without any "omnibus" legislation. Thus, for example, in the U.S., a number of professional groups and industrial associations have adopted codes of ethics which include provisions for the protection of personal data these include the American Medical Association Code of Ethics, the American Bar Association Code of Ethics, the Institute for Certification of Computer Professionals Code of Ethics, and so on*2.

Furthermore, various companies and organizations in the OECD member countries voluntarily adopted codes of conduct which reflect the principles commonly contained in the OECD Guidelines and the CoE Convention. As of March 1983, 182 corporations based in the U.S. had adopted or planned to adopt policies based on the OECD Guidelines*3. In December 1986, the Canadian Secretary of State for External Affairs wrote to approximately 150 major private Canadian corporations recommending the OECD Guidelines to them and urging them to develop and implement privacy protection codes consistent therewith, and in response to this recommendation, the Canadian Banker's Association issued a model privacy code in June 1987*4. In Japan, as will be referred to later [sec. 4.3.2], government encouragement of the use of the OECD Guidelines as a model has led to the publication by financial institutions in March 1987 of a set of voluntary guidelines for the protection of personal data*5.

4.1.3 Development of International Industry Recommendations

Moreover, the development of international industry recommendations can also be observed. The International Air Transport Association (IATA) is the trade association of the world's scheduled airlines and is made up of some 160 airlines from over 100 countries. Thus, the number of related

telecommunications messages generated by IATA carriers exceeds 11 billion a year. Because of the growing magnitude of its task, IATA has perceived the difficulties of trying to meet the various standards of data protection which prevail in many of the countries where IATA members operate. In order to assist its members having difficulties complying with such varying standards of data protection, IATA has recommended to its members the adoption of the procedures set out in a document entitled "Protection of Privacy and Transborder Data Flows of Personal Data Used in International Air Transport of Passengers and Cargo", which was adopted at the IATA Passenger Services Conference in September 1987*6.

The IATA recommendation covers any information relating to an identified or identifiable individual which would include passenger flight details and baggage information, and only apply to automated personal data files. Three principles are set down quality of data, data security; and additional data safeguards. These principles reflect the spirit of the OECD Guidelines and the CoE Convention, although not their actual provisions. The IATA recommendation will prove extremely useful when its members operate in countries which lack certain measures for personal data protection. Especially in these circumstances, the recommendation will make a positive contribution. Such recommendations or codes of conduct may also have the effect of promoting customer confidence in the

services offered so that there may be favourable commercial implications.

4.1.4 General Support for the Development of Voluntary Protection Regimes

Judging from the answers to a questionnaire sent to OECD member countries by May 1988 for the preparation of the fourth ad hoc meeting on the follow-up of the OECD Guidelines, a large majority of member countries favoured the development of codes of conduct modeled on the principles set out in the OECD Guidelines and the CoE Convention as the approach to self-regulation. In countries where there is existing data protection legislation, voluntary codes of practice are seen as a fine-tuning mecnanism which supplement the practical application of the general principles of the legislation in a particular sector or organization. It must be added however that voluntary codes of conduct unsupported by legislation do not provide data subjects with inviolable rights against data users, which drawback must always be taken into consideration whenever the voluntary regulatory approach is taken.

4.1.5 The CoE's Elaboration of Non-Binding Sectoral Standards

Interesting enough, this "bottom-up" trend is even influencing the stance of the CoE which once had led the "top-down" approach for European countries.

Following elaboration of the CoE Convention, the inter-governmental Committee of Experts on Data Protection turned its attention to a sectoral approach to data protection problems. The Committee considered that the general principles provided in the CoE Convention could be the subject of detailed application to certain identified sectors, taking account of the nature of problems specific to data processing in a particular area. That is, for example, the basic principle that data shall be obtained and processed fairly and lawfully may be applied differently for medical data as for direct marketing data.

With this approach in mind the Committee has so far drawn up non-binding legal instruments, i.e. "recommendations", for six sectors which have subsequently been adopted by the Committee of Ministers. These recommendations are as follows:

1. Recommendation No.R(81)1 on regulations for automated medical data banks,
2. Recommendation No R(83)10 on the protection of personal data used for purposes of scientific research and

statistic,

3. Recommendation No.R(85)20 on the protection of personal data used for purposes of direct marketing,
4. Recommendation No.R(86)6 on the protection of personal data used for social security purposes,
5. Recommendation No.R(87)15 on the protection of personal data used in the police sector,
6. Recommendation No.R(89)2 on the protection of personal data used for employment purposes.

The Committee of Experts on Data Protection is currently examining the data protection problems posed by the banking sector and by electronic payments in particular*7.

Concerning these CoE recommendations, Mr. T.L. Early, the CoE Directorate of Legal Affairs comments as follows:

> [T]hese are non-binding legal instruments -- they are recommendations -- setting out a framework of data protection rules for the different sectors examined and which are addressed to the governments of the [CoE] member states in the hope that the solutions put forward will be taken up in the domestic law and practice of member states when they are faced with problems of the kind covered by each of the instruments*8.

4.2 Convergence of Legislative Approaches to TDF

4.2.1 Moderation of Restrictions on TDF

As of April 1988, although nine of the twelve OECD member countries have national data protection legislation with provisions relating to TDF, the nature of these provisons vary widely. This is obviously an area of some importance which may have an impact on international trade in services. Some states treat transborder data flows as just another aspect of the transfer of personal data so that no special requirement exists in relation to it, that it must be treated in the same way as all other personal data. This approach has been taken in Germany*9 and Japan*10 for example.

Austria, on the other hand, requires in certain circumstances that the data user or collector be granted a licence before any personal data is transmitted. Recent amendments have reduced the number of occasions upon which a licence must be sought. In Austria, where a system of notification and registration for the public and private sectors exists, the legislation has been amended to simplify the registration procedures, especially for transborder flows of personal data. The effects of these changes are as follows:

1. No special licence is required for TDF where the personal data is sent to a country offering

equivalent standards of protection,

2. If no equivalent protection is offered, then a licence for the transmission will only be given where

i) The transmission takes place according to bilateral or multilateral agreements which expressly mention the categories of data and their destination;

ii) The data subject has granted his/her written consent to the transmission;

iii) The data has already been published legally in Austria, or

iv) The data constitutes a standard transmission and the Federal Chancellor in consultation with the Data Protection Council decides above all that the data contains no private information that requires protection. For example, standard transmissions by airline companies fall into this category.

3. In all other cases a licence must be obtained before any transborder flow of personal data occurs^11.

France, Finland and Norway permit the free flow of international personal data subject to the overriding discretionary power of the relevant authority to prohibit or regulate such activity^12.

By contrast, in Sweden and Iceland, generally permission of

the data protection authority is required before any international transfer of personal data which falls within one of the categories under the legislation*13.

Generally it can be expected that as more countries ratify the CoE Convention, the data protection laws concerning TDF in CoE member countries will become similar because they all must agree with the provisions of article 12 of the CoE Convention. This process of integration may continue in the European states as they head towards a common market in 1992. This underscores the problems which non-European states that lack comprehensive data protection laws may face when trading with European states. Actually non-European common law countries (Australia, Canada, New Zealand and the United States) which do not have such provisions may suffer adverse consequences when entering into trade in data services where the country in which the other trader resides has data protection laws which prohibit the transfer of personal data to countries without equivalent protections. Moreover, at the second meeting of the Consultative Committee of the CoE Convention held in May 1988, it was reported that a question receiving some attention from the contracting European countries had to do with how states were applying the requirement of "equivalent treatment" of protection of local data transferred outside their jurisdiction*14.

However, although no major study has been undertaken in

this area, in the answers to a questionnaire sent to OECD members in 1987 for the preparation of the fourth ad hoc meeting, no cases have been provided showing that transborder data provisions have substantially impeded international trade in data services. This position has been suppoted by a recent survey in the United Kingdom, which indicated that companies involved in these activities were more concerned about domestic registration requirements than restrictions on the transborder flows of personal data*15.

4.2.2 Transformation of the Problematic Stages from "'Legal Person' Privacy" to "Business Communication"

In 1983, the Second OECD Symposium on TDF was organized in London, with 250 participants from 20 OECD members, and observers from a dozen international organizations. In the welcoming address, Mr. H.-P. Gassmann, head of the OECD Committee on Information, Computer and Communications Policy (ICCP) Secretariat, called attention to the fact that, having passed the "privacy" stage in the evolution of TDF issues, the OECD member countries have entered the "business communication" stage*16. As the result of the 1983 TDF Symposium, in order to examine the strategic importance of non-personal TDF for international economic transactions, the ICCP Committee and the

Working Party on TDF met regularly and sought to promote the idea of a TDF Declaration, as a set of international principles governing non-personal TDF. After three-years of negotiations, the Declaration on Transborder Data Flows*17 was formally adopted by the OECD Council of Ministers on 11 April 1985.

The Declaration, although not legally binding, recognizes the increasing economic importance of TDF, and affirms that OECD member countries have a common interest in facilitating TDF, and in reconciling different policy objectives in this field in order to establish transparent and stable policies, regulations and practices for investment and trade. It also declares the member countries' intention to consult with each other and consider the implications for other states before taking action relating to non-personal TDF of following kinds:

1. data accompanying international trade
2. marketed computer services and computerized information services
3. intra-corporate data flows*18.

Although the four European states mentioned in Chapter 2 [sec. 2.2.2.2] currently include both natural and legal persons in the "data subject" sections of their data protection legislation, the most recent European data protection laws in Finland, the U K., Ireland and Netherland which are called "second-generation" legislation*19, and the provisions of the Greek and Portuguese bills indicate that the trend extends to

the protection of natural persons only*20.

And even under the existing provisions for the protection of "legal person" privacy, a potential administrative solution to the conflict between some level of protection of small firms' privacy and confidentiality of corporations' commercial information. In Norway, IBM applied for an exemption from the "legal person" application of the Personal Registers Act of 1978, claiming if customers and competitors gained access to IBM's files, its marketing activities would be damaged. In February 1983, Norway's Data Inspectorate (DI) granted IBM an exemption concerning access, on condition that the DI retained the right to intervene and maintain the law if a complaint was received*21. It may be presumed that, as IBM had declared its compliance with the OECD Guidelines*22, some accommodation could be reached with Norway being a member of the OECD.

From the foregoing, it can be seen that a consensus has arisen among European countries that the protection of the confidentiality of data concerning business legal persons by legislation designed to protect the privacy of natural persons, is "inappropriate, unnecessary, and potentially harmful*23."

4.3 Its Influence on the Japanese Public and Private Sectors

4.3.1 The Japanese Public Sector

4.3.1.1 The 1988 Act for Protection of Computer-Processed Personal Data held by Administrative Organs

Until recently, the social and thus the legal concept of "privacy" was not much accepted in Japan, like other Asian societies under the influence of Buddhism and Confucianism. This is perhaps because, unlike people in Western countries, Japanese people traditionally were not baptized with the idea of individualism originated in the philosophy of the Greeks. However, along with the widespread use of computers in society, and the accompanying increase in the risk of infringement on the rights and interests of individuals by the misuse of processed personal data, an awareness of, not to mention and concern about, "data privacy" has been fostered among Japanese people also. Therefore to provide fundamental rules for the handling of computer-processed personal data, so as to eliminate citizens' anxiety, discussions concerning both the scope of and specific provisions of data protection legislation had been held by the Diet, the academic, media, labor and citizens' groups since the early 1970s. Two further reasons

also contributed to this increased discussion, namely, the enactment of data protection legislation in one Western country after another, and the increase in the number of Japanese local ordinances to protect persoanl data*24, expedited the enactment of national legislation for personal data protection. In particular, the adoption of the OECD Guidelines pressured the Japanese government (Japan being a member state of the OECD) to rush to enact national data protection laws. For example, a study paper entitled "The Status Quo and the Future of the Protection of Privacy Measures for the protection of privacy regarding computer-processed personal data", which was published in 1982 by an advisory study group appointed by the Management and Coordination Agency with cooperation of Ministry of Justice, spends one chapter examining the rules of the OECD Guidelines, whereas the Japanese translation of the CoE Convention is provided merely as a reference material in the report's Appendix*25.

In fact, based on this study paper, section 4(2)(i) of the decision of the Japanese Cabinet Meeting of 29 December 1984 confirmed the need for legal measures for the protection of personal data held by administrative bodies "taking into account the present situation [concerning the protection of personal data] in foreign countries"*26. Finally, the Act for Protection of Computer-Processed Personal Data held by Administrative Organs (hereinafter the Act) was given the

Diet's approval on 9 December 1988 and promulgated on 16 December 1988*27.

The contents of the Act are generally the same as above those of the other data protection laws indicated in Chapter 2 [sec. 2.1.2] the purpose of the Act is to protect individual rights and interests while promoting the proper and smooth functioning of public administration [art. 1], the Act requires that the government adopt a purpose limitation approach in its collection of and exchange of information between government departments [art. 4], each ministry and agency of government must inform the The Director-General of the Management and Coordination Agency (DG/MCA) of the kind of information being collected and the purpose for collection, with several exceptions, e.g. the files about the state security, criminal information, public servant personnel records [art. 6]; and the DG/MCA must make public at least once a year these details [art. 8], individuals will have access to his/her information, with several exceptions, e.g. the files about school records, medical information, and criminal information of the person [art. 13], and will be able to petition for correction, although he/she has no automatic legal right to correct the relevant information [art. 17].

4.3.1.2 Influence of the Two Organizations' Achievement on the Act

Mainly influenced by the activities concerning the OECD Guidelines with the enough lessons of "first generation legislation", i.e. the data protection legislation of Western countries in the 1970s and early 1980s, the Act bears the characteristics of the "second generation legislation"*28. In particular, with regards to the three points in the previous sections [secs. 4.1 and 4.2], the impact of the OECD Guidelines are quite clear.

Firstly, regarding the adoption of "bottom-up" approach, or its alternative expression in the public sector as the simplification of data protection procedures, for reducing the administrative burden, the Act does not have an independent personal data supervisory body. Instead, the DG/MCA is fulfilling almost the same role as a supervisory body by receiving prior notification of personal data files from each government ministry and agency, and by exercising authority invested in it by the Act to supervise the heads of those administrative bodies for the execution of the Act. Additionally the Act has a provision directly promoting the "bottom-up" approach even in the public sector, namely article 27 regarding the responsibility of special public corporations towards the protection of personal information. As at the end

of June 1988, processed personal data held by the 54 special public institutions (that is, bodies whose creation was the sole purpose of the laws setting them up, e.g. the Small Business Credit Insurance Corporation, the Housing Loan Corporation, Kokusai Denshin Denwa Corporation (KDD), the Central Cooperative Bank for Agriculture and Forestry, and the Japan Broadcasting Corporation (NHK)), has reached a total of 237 files, or about 200 million pieces of information. Considering this situation, the article requires these special public institutions to take the necessary measures to secure the proper handling of personal information "voluntarily, following and/or consulting the rules of the Act"*29.

Secondly, nor are provisions on TDF regulation to be found in the Act. This was a deliberate choice on the part of the Japanese authorities, in the light of the European trend of relaxing restrictions on TDF, and of the fact that there have been no cases of infringement of personal data privacy concerning the files held by Japanese administrative organs*30. On the issue of so-called "data havens", it is also worth noting that, unless there is a particular reason for the contrary, the Act applies equally to the personal information held by Japanese government institutions concerning foreign nationals*31. This consequence resulted from a fundamental recognition that, "under the OECD Guidelines and other instruments", for the reconciliation of the demands of privacy

protection and of free transborder flows of personal data, it is inevitable to ensure that there is no unfair discrimination against data subjects due to nationality or residence*32.

Thirdly concerning provisions on the privacy protection of "legal person", i.e. incorporated entities, the Act seems to incorporate certain the result of lessons drawn from the achievements of the OECD and the CoE. In principle, the Act applies only to natural persons in the light of its purpose to protect the rights and interests of individuals, thereby placing corporations and any other bodies whether or not such bodies possess legal personality out of its scope.

Nevertheless, however, some pragmatic exceptions can be observed.

Firstly, according to the commentary concerning definition provision of the Act, which was compiled under the supervision of the Administrative Management Bureau of the MCA, the definition of the term 'personal information" contains the business information of a sole proprietor who carries on a one-man business, thereby bringing such individuals' business information within the protection of the Act*33. This clause was included because it was considered impossible to distinguish between personal information and business information of an individual carring on a one-man business, and thus that, such individuals should also be protected by the Act. Therefore with respect to business information,

application of the Act depends on whether the data subject which carries on the business in question, is an individual or a corporation or other incorporated body*34.

Secondly, the Act deliberately stipulates the treatment for so-called "mixed 'legal person' files" which are the files incorporating personal information as well as business information under article 2 (2). In order to protect the rights and interests of individuals, all computer-processed personal information, even in the "legal person" files held by administrative organs, is to come under the scope of the Act. Thus, for example, in the case of a file held by Legal Affairs Bureau of Ministry of Justice, which stores the computer-processed firm register records required under section 64 (1) of the Commercial Code*35, the Code's application extends to the personal information of employees and investors. On the other hand, when the securities registration statement of a corporation, required under article 24 of the Securities and Exchange Act *36 contains the names, titles, birth dates, addresses, brief personal histories, and numbers of holding stocks of the directors of that corporation, these pieces of "personal" information of the directors are beyond the scope of the Act, since they are regarded as the "business" information concerning the directors as the "organs" of that corporation.

4.3.2 The Japanese Private Sector

4.3.2.1 The Regulations Aimed at the Private Sector in Japanese Legislation after the Adoption of the Two International Instruments

While the Japanese government has encouraged the use of the OECD Guidelines by industry*37, it has also continued research projects for the development of national privacy laws for the private sector, following the Decision of the Cabinet Meeting of 29 December 1984*38.

Although Japan has not yet enacted a comprehensive set of national data protection laws for the private sector, there are several regulations for that purpose which were enacted or amended after the adoption of the two international instruments.

In the Regulation of Money-Lending Businesses Act*39, article 25 provides that, by the each prefecture credit industry association, self-imposed standards of appropriate behavior for the industry should be established. Each association shall direct the member credit firms not to make loan contracts which would exceed a debtor's capacity to repay and to give the relevant information to the member firms by establishing or designating a credit agency which operates to collect information on the credit-worthiness of debtors [art.

30(1)]. Article 30 (2) further prescribes that the member firm shall not use the personal data collected by a credit agency, for any purpose other than for obtaining information about a debtor's capacity to repay. Also the Hire-Purchase Act*40 has the same kind of provisions concerning the appropriate treatment of customers' information in the case of instalment repayments and the relevant credit agencies [arts. 42.2 - 42.4].

Based on articles 45 and 46 of the Regulation of Money-Lending Businesses Act, on 4 March 1986, the Director of Regional Finance Bureau, who was delegated the authority concerned by the Minister of Finance, issued a circular concerning the protection of personal confidential information in the financial industry*41. The mandate of this circular has, as mentioned before [sec. 4.1.2], led to the publication of the "Guidelines on the Protection of Personal Data for Financial Institutions" of March 1987 by the Financial Information System Center (FISC), an affiliated body of the Ministry of Finance. Similarly, based on articles 47 and 48 (1) of the Hire-Purchase Act, on 4 March 1986, the Director of Industrial Policy Bureau of the Ministry of International Trade and Industry (hereinafter MITI) issued a circular regarding the proper management of consumer credit information in the consumer credit industry*42, a part of its mandate later produced the voluntary registering system of data-protection

codes adopted by private corporations, which has been promoted by MITI, as mentioned below.

4.3.2.2 Influences of the Two Organizations' Achievements on the Self-Imposed Standards Set by the Japanese Private Sector

After the enactment of the 1988 Act for the public sector, certain legal measures for the protection of personal data in the private sector were strongly demanded by industry. Responding to the demand, the Cabinet Meeting of 24 January 1989 decided that more positive measures should be taken in the private sector, and to that effect Cabinet required relevant ministries to take the necessary steps*43.

By that time, the Japan Information Processing Development Center (JIPDEC), an affiliated body of MITI, had already published its model guidelines, namely the "Guidelines to Protect Personal Data in the Private Sector" whose contents were based on the rules of Part Two of the OECD Guidelines, i.e. the basic principles of national application. MITI circulated these JIPDEC guidelines to leading industry associations under its jurisdiction, encouraging them to establish proper guidelines for their respective industries giving consideration to its particular circumstances. Then, on 18 April 1989, MITI released the "Regulations on the Register

of Measures to Protect Personal Data Processed by Computers" (hereinafter the MITI Regulations)*44.

The MITI Regulations aim to encourage the private sector to take the necessary measures to protect processed personal data held by private corporations, and thereby to contribute higher standard of living for consumers, by means of a system of registering data-protection measures for consumers' inspection [para. 1]. The corporations "may notify" MITI of following information: description of the corporation's operation; outline of the measures for personal data protection; and reference address from consumers' inquiries, and MITI will compile those pieces of information for consumers' inquiry [paras. 3 and 4]. Although the MITI Regulations do no more than urge private corporations to register voluntarily, considering the recognized power of administrative direction, or gyousei-shidou in Japanese, the MITI Regulations may be able to demonstrate considerable binding power for the Japanese private sector*45.

The FISC's "Guidelines on the Protection of Personal Data for Financial Institutions" of March 1987 also originated from the mandate of a circular issued by the Ministry of Finance. The FISC Guidelines are therefore recognizing, along with the JIPDEC Guidelines under the MITI Regulations, the advantages of the "bottom-up" approach in the CoE style which provides on the one hand a legally enforceable regime for data protection and

on the other, allows a certain degree of self-regulation in the form of the development of rules appropriate to respective private sectors. And, as found in the contents of the FISC Guidelines*46, the "core" standards of these self-imposed rules are strongly influenced by the common rules for domestic application found in both the OECD Guidelines and the CoE Convention which were examined in Chapter 3 [sec. 3.1.3].

Footnotes to CHAPTER 4

*1 Those seven countries are Austria, Denmark, Finland, France, Iceland, Norway and Sweden. The information was provided during an interview in June 1988 with Mr. Muramatsu of MCA who in turn obtained the information from the OECD document [DSTI/ICCP/88.5].

*2 Briat, supra, CHAPTER 3 note 26 at 369.

*3 Id. at 389ff.

*4 This model privacy code by Canadian Banker's Association was presented, at the fourth OECD ad hoc meeting in 1988, as an example of use of the OECD Guidelines in banking industries. The information was provided during an interview in June 1988 with Mr. Muramatsu of MCA who in turn obtained the information from the OECD document [DSTI/ICCP/88.8].

*5 This voluntary guidelines in Japanese finance industries by Center for Financial Industry Information Systems (FISC) was also presented at the fourth OECD ad hoc meeting in 1988 [OECD Doc. DSTI/ICCP/88.7] , This FISC Guidelines are contained in ANNEX 6 of this thesis.

*6 The IATA recommendation is reprinted in: W. Monssen, "Airline Industry Takes Data Protection Seriously" (January 1988) 11 T.D.R. 17 at 19.

*7 P.J. Hustinx, "COE and Data Protection: What has been achieved?" (November 1989) 12 T.D.R. 21 at 22.

*8 T.L. Early, "Recent Developments in Data Protection in the Council of Europe" (November/December 1986) Computer Law & Practice 68 at 69.

*9 See "Registrations -- How Much First-Year Success?" (August 1986) 9 T.D.R. 25 at 25 [hereinafter Registrations]; see also "Data Commissioners Assess Privacy Threats" (October 1987) 10 T.D.R. 10 at 13 [hereinafter Data Commissioners].

*10 See sec. 4.3.1.2 of this thesis.

*11 See "Austria: Deregulation of privacy act in parliament" (May 1986) 9 T.D.R. 24; see also "Austria: TDF experiences reported" (February 1987) 10 T.D.R. 24.

*12 See Registrations, supra, note 9 at 26; "Norway : Reforms proposed" (July 1987) 10 T.D.R. 23; and K. Selmer, "Data Protection Policy Trends" (December 1988) 11 T.D.R. 19.

*13 "Sweden's Transborder Data Flow Experiences" (November 1989) 12 T.D.R. 9; Data Commissioners, supra, note 9 at 10.

*14 Supra, CHAPTER 3 note 28.

*15 These comments were provided during an interview in June 1988 with Mr. Muramatsu of MCA who in turn obtained the information from the OECD document [DSTI/ICCP/88.5].

*16 C.R. Pipe, "Searching for Appropriate TDF Regulation" (January/February 1984) 7 T.D.R. 1 at 2.

*17 TDF Declaration, supra, CHAPTER 1 note 10.

*18 Sauvant, supra, INTRODUCTION note 5 at 242.

*19 The term "second-generation" legislation has been used to indicate a number of data protection laws, notably those of Finland (enacted in 1987) and the Netherlands (enacted in 1989).

The term is derived from the computer industry where it is used to describe the second stage of development of computers. Mr. P. Hustinx, legal adviser in the Dutch Ministry of Justice, and chairman of the CoE Committee of Experts on Data Protection, observed "second-generation" data protection laws as having a number of characteristics: it covers a wider range of material, mainly relating to manual records; there is a trend towards simplification; a greater amount of differentiation for the sectors; a trend in favor of self-regulation, and the increased use of informal and civil sanctions as a means of enforcing data protection. See "Data

Protection Responding to Trends in Technology" (January 1988) 11 T.D.R. 12 at 12, see also, V.A. de Pous, "Dutch Data Protection Act in Force" (December 1989) 12 T.D.R. 21.

*20 Switzerland is currently considering a bill on data protection which would include legal persons. Walden & Savage, supra, CHAPTER 2 note 23 at 337-338.

*21 Id. at 346.

*22 Briat, supra, CHAPTER 3 note 26 at 390.

*23 R.V. Austin, the International Chamber of Commerce (ICC), Address (The first meeting of the European Legal Observatory, 1985). Cited from: "Legal Person Privacy Debate in Europe" (January 1986) 9 T.D.R. 3 at 3.

*24 As of April 1989, a total of 572 Japanese cities, towns and villages have enacted ordinances for personal data protection ["National Reports, Japan" [Special Report of the 11th Annual Data Commissioners Conference, 29 August - 1 September 1989] (November 1989) 12 T.D.R. 14 at 14]. The Japan's Personal Data Protection Act of 1988 is seen as contributing to the co-ordination of the various measures enacted by prefectural and municipal governments.

*25 Administrative Management Bureau, Administrative Management Agency (renamed later the "Management and Coordination Agency") ed., The Status Quo and the Future of the Protection of Privacy: Measures for the protection of privacy regarding processed personal data (published in Japanese) (Tokyo: Gyousei, 1982).

*26 The Decision of the Cabinet Meeting of 29 December 1984, Japan, Kanpō(the official gazette), No.17375 at 13 (10 January 1985) [hereinafter Cabinet Decision of 29 December 1984], reprinted in: The Administrative Management Bureau of the MCA, The Personal Data Protection Act and its Commentary (published in Japanese) (Tokyo: Daiichi-hōki, 1989) at 254[hereinafter

Commentary..

*27 Act for Protection of Computer-Processed Personal Data held by Administrative Organs 1988 (Japan), c. 95. The Act came into force in October 1989. The unofficial translation of the full text of this Act is contained in Annex 5 of this thesis (reproduced from "Japan Adopts Privacy Protection Act" (February 1989) 12 T.D.R. 26 at 26ff...

*28 See, Supra, note 25.

*29 Commentary, Supra, note 26 at 224-225.

*30 These comments were provided during an interview in June 1988 with Mr. Muramatsu of MCA.

*31 Commentary, Supra, note 26 at 69.

*32 Ibid.

*33 Commentary, supra, note 26 at 68.

*34 Ibid.

*35 Commercial Code 1899 (Japan) c. 48, later amended by 1981 (Japan) c. 74.

*36 Securities and Exchange Act 1948 (Japan) c. 25, later amended by 1965 (Japan) c. 1...

*37 "Japan. Search for appropriate measures continues" (May 1986) 9 T.D.R. 24.

*38 Cabinet Decision of 29 December 1984, Supra, note 26, sec. 4(2)(1).

*39 Regulation of Money-Lending Businesses Act 1983 (Japan) c. 32, later amended by 1983 (Japan) c. 33 and c.78.

*40 Hire-Purchase Act 1961 (Japan) c. 159, later amended by 1964 (Japan) c. 25, 49, and 1988 (Japan) c.109.

*41 "Proper Data Management Circular in Financial Industry by MITI & Ministry of Finance" (published in Japanese) The Japan, Nihon Keizai Shinbun (5 March 1986) 3 (hereinafter Circular). For the detailed contents of this circular of 4 March 1988, see T. Hiramatsu, "Japan's Private-sector Data Protection" (May

1990) 13 T.D.R. 11 at 11.

*42 Circular, supra, note 41.

*43 Sec. 8(1)(i), the Decision of the Cabinet Meeting of 24 January 1989, Japan, Kanpo(the official gazette), No.14 at 12 (16 January 1989).

*44 "Setting Self-Regulatory Rules for Privacy Protection. the MITI Regulations Released" (published in Japanese) The [Japan] Nihon Keizai Shinbun (19 April 1989) 1. For the detailed contents of the MITI Regulations, see T. Hiramatsu, supra, note 41 at 12-13.

*45 T. Hiramatsu, supra, note 41 at 13.

*46 See ANNEX 6 of this thesis.

CHAPTER 5.

Conclusion: Effective Regulatory Techniques in the Field of Telematics

5.1 Definition of the Focus and Method of this Study

Based on an evaluation of the two organizations' achievements, it may now be considered what the international regulatory techniques governing TDF should be. In order to define the focus of this study, it is first necessary to look at some of the features of the consequences concerning the OECD Guidelines and the CoE Convention.

The OECD Guidelines are not binding, but this fact does not necessarily diminish their impact, if there is a political will on the part of the member states to give effect to them. They are the rules of conduct to which member states agree to conform. Moreover, for the sake of their voluntary nature, The OECD Guidelines are obeyed not only to the member states, but also to other entities, such as international organizations and multinational enterprises. States like the U.S., Canada, and Japan, which do not have laws regulating data privacy protection in the private sector, viewed The OECD Guidelines as a set of standards endorsed by the European states. Those countries without data protection legislation aimed towards their private sectors would thereby prevent unnecessary or

discriminatory restrictions on their corporations' information activities even in Europe, if those corporations were to follow the standards of The OECD Guidelines voluntarily. Generally, through all the steps taken by the OECD in relation to the OECD Guidelines, the emphasis has been placed on voluntary action and a pragmatic rather than an overly legalistic approach to the problems. Particularly, the emphasis has been put on follow-up procedures which bring the results of cases of actual application to the OECD to check the member states' implementations of the OECD Guidelines and negotiate for the development of further harmonization of their positions which were at the outset markedly divergent.

On the other hand, with respect to measures taken by the CoE under the CoE Convention, the following three points can not be ignored, although, to date, it is still not easy to estimate the degrees of effectiveness of the OECD Guidelines and the CoE Convention because of several reasons as mentioned in Chapter 3[sec. 3.2]. Firstly, following its adoption, it was some five years before the CoE Convention came into force, whereas the OECD Guidelines applied immediately by each member state respectively from the time when adopted*1. Further, the body responsible for its implementation, the Consultative Committee started to operate substantially from 1988, eight-years after the adoption of the CoE Convention. Secondly, even among the follow-up actions taken under the CoE

Convention which is a traditional-legally binding treaty, non-binding self-regulatory measures such as codes of conduct have been later recommended, to allow different industries a certain degree of fine-tuning of data protection standards. Moreover, thirdly, according to Mr. P.J. Hustinx, a former chairman of the CoE Committee of Experts on Data Protection, apart from the preparation of those Recommendations and studies on specific subjects, the Committee of Experts has proven to be a valuable forum for the exchange of information for government representatives working in the field of data protection*2.

Given these consequences of the adoption and implementaion of the two instruments, for the purpose of any discussion regarding the international regulatory techniques governing TDF, the focus can be put on the common regulatory techniques of the measures taken under the OECD Guidelines and the CoE Convention, such techniques being namely the practice of combining adoption of non-binding principles and standards with collective follow-up procedures. The discussion in this chapter deals mainly with the activities concerning the OECD Guidelines for the following reasons: firstly, the legislative approaches on data protection are converging in favor of the "bottom-up" approach of the OECD Guidelines, as examined in Chapter 4 [sec. 4.1]; secondly, the follow-up activities under the CoE Convention have not yet accumulated to allow adequate analysis. Although the discussion is in principle based on the

findings made in the preceding chapters, for the purpose of a more detailed analysis, the practices concerning other OECD Guidelines in the fields of international investment and multinational enterprises will also be mentioned.

5.2 The OECD Guidelines as "Soft Law": Their Legal Effect and Shortcomings

Notwithstanding the effectiveness of the OECD Guidelines in reconciling competing national policies on TDF, they are explicitly stated to be voluntary and not legally enforceable. That is the reason why the OECD Guidelines are called "soft law", in accordance with their proclaimed non-binding nature. This concept of "soft law" in international law has been familiar since the early 1970s, although its precise meaning is still the subject of much debate*3.

As it is outside the purpose of this thesis to examine and discuss the legal nature of "soft law", the following assertions about "soft norms" by the late Judge R.R. Baxter will be helpful to comprehend the "legal effect" of the OECD Guidelines as "soft law". Cautioning explicitly that generalizations are difficult because of the different "legal impact"*4 of each respective "soft" instrument, he enumerates the supportable assertions as follows:

1. If some sort of written norm has been consented to by the States involved, the future course of discussion, negotiation, and even agreement will not be the same as they would have been in the absence of the norm.

2. Once a matter has become the subject of such a norm, the matter can no longer be asserted to be one within the reserved domain or domestic jurisdiction of the State. As the Permanent Court said in its advisory opinion on Nationality Decrees Issued in Tunis and Morocco, "the question whether a certain matter is or is not solely within the jurisdiction of a State is an essentially relative question; it depends upon the development of international relations" [1923 P.C.I.J., ser.B. No.4 at 24]. And one way in which international relations develop is through agreement.

3. The norm will establish new standards of relevance for the negotiations between the parties. Certain arguments will be ruled out. Economic considerations, under Article 5 of the Definition of Aggression adopted by the General Assembly [G.A.Res. 3314(XXIX), 29 U.N.GAOR Supp. No.31 at 143, UN Doc.A/9631 (1975)] after so much travail, are ruled out as a possible justification for the use of force against a State. That clearing of the ground is helpful, even though the definition may not be of material assistance in determining whether an act

of aggression has taken place.

4. The norm will establish the legal framework within which the dispute about its application may be resolved. It will establish presumptions, indicate the prevailing trend of opinion, provide a guiding principle which may have a certain inherent appeal for the parties, and channel negotiation and settlement into legal and orderly paths*5.

However, despite of this considerable influence, "soft law" does have certain disadvantages: for example, the rules of the OECD Guidelines can not as such be sanctioned by any court or tribunal at either a national or international level, where either not all the parties to a given conflict have previously accepted them, or where some parties interpret the content of those rules in a different manner. Furthermore, objectively, non-observance of the OECD Guidelines can hardly qualify as international delinquency, which means that a state affected by such non-observance would not be entitled under international law to resort to reprisals, namely, "to objectively illegal acts, which international law renders nonetheless legitimate as retaliation against a violation of (hard) rules of international law*6."

Nevertheless, as analyzed in Chapter 4, the OECD Guidelines demonstrated their power of "community engineering"

and promoted the harmonization of national legal policies on TDF. It is therefore reasonable to predict that, instead of any strict compulsory measures, certain mechanisms to foster member states' compliance will be devised within the existing institutional framework governing the OECD Guidelines.

5.3 Two Functions of the Institutional Mechanism Governing the OECD Guidelines: the Follow-Up Procedures

5.3.1 Improving Acceptability of the Rules by Feedback Information Gained from Practical Application

It is certain that a set of rules called the OECD Guidelines does not create legal rights nor enforceable obligations. However, The OECD Guidelines have "persuasiveness", and therefore in turn, "acceptability", as the minimum common level of enforcement that was reached through negotiations between the various entities with an interest in the field of TDF. More particularly, this field, called the "TDF problems", gives rise to broader issues whose features and contents have changed rapidly with the advance in technological development of informatics and telecommunications. In these circumstances, ad hoc meetings on the follow-up of the OECD Guidelines at which specific

information and the views of member states are exchanged, have proved useful. As mentioned in Chapter 4 [sec. 4.2.2], at the second OECD ad hoc meeting of 1983, the member states had already come to recognized that no law, policy nor procedure concerning the protection of personal data was found to create obstacles to the transborder movement of personal data. At the fourth meeting of 1988, the most recent developments of data protection legislation were introduced, i.e. so-called "second generation" legislation which had been drafted on the basis of the OECD countries' experiences in the 1970s and early 1980s*7.

Furthermore, when information obtained by member states from their national implementation of the OECD Guidelines is fed back to the follow-up meetings, it may bring about refinement of existing rules which are better suited to changing circumstances and accordingly more acceptable to member states. In fact, a pertinent example of the development of further standards by feedback action can be observed in the measures taken by the OECD in the field of international investment and multinational enterprises.

On 21 June 1976, the OECD member states, agreeing "to take measures designed to improve the investment climate" and recommending that "multinational enterprises should abide by certain standards of behaviour set forth in a series of guidelines*8", adopted "the Declaration on International Investment and Multinational Enterprises"*9.

The outlines of the Declaration are as follows:

1. A recommendation to multinational enterprises operating in the member states' territories to observe the Guidelines for Multinational Enterprises (hereinafter the 1976 Guidelines);
2. The principle of national treatment, namely the accordance by member states to multinational enterprises operating in the member states' territories and owned, or controlled, directly or indirectly, by nationals of another member state;
3. A statement on international investment incentives and disincentives;
4. Consultation procedures, namely that the governments of member states are prepared to consult one another on the above matters in conformity with the relevant OECD Decisions;
5. A statement on the Review of the Declaration. The governments of member states will review the above matters at the latest in five years with a view to improving the effectiveness of international economic co-operation among them on issues relating to international investment and multinational enterprises.

According to paragraph 5 of the Declaration and to

Decision C(76)117*10 of the OECD Council on Inter-Governmental Consultation Procedures on the Guidelines for Multinational Enterprises (the 1976 Guidelines), when the ministers of the member states met at the OECD headquarters in Paris, on 13-14 June 1979, they reviewed their cooperation in the field of international investment and multinational enterprises*11.

Regarding the 1976 Guidelines, one change in paragraph 8, was adopted to cover the situation where workers were transfer from a foreign affiliate in order to influence unfairly negotiations with employees, an issue which had not been foreseen when the 1976 Guidelines were drafted*12.

At the same time, the follow-up procedures of the 1976 Guidelines under the text of the Decision C(76)117 were changed and brought into greater conformity with the practices of the central body organizing this project. the OECD Committee on International Investment and Multinational Enterprises (hereinfater the IIME Committee)*13, whose practice has evolved since 1976*14.

Prof. Blanpain comments on the 1979 amendment of the 1976 Guidelines as follows·

> The text of [the 1976 Guidelines] was, for the sake of credibility and stability, only slightly amended, to cover an issue that was not foreseen when [the 1976 Guidelines] were drafted. It was accepted by most that the 1976 deal

constituted a fragile package, the delicate balance of which had to be maintained. The credibility -- in the sense of stability -- of [the 1976 Guidelines], required that after such a short period no changes should be made. The one change, obviously again a compromise, since more changes were asked for, indicates that changes which are needed are possible, which is also necessary for the same 'credibility'*15.

With respect to the OECD Guidelines, throughout four ad hoc meetings concerning their follow-up, their wording was not changed. However, "changes which are needed seem to be possible" as observed above under the 1976 Guidelines, if a problem that was not expected at the time of drafting occurs. And the role which the IIME Committee played under the 1976 Guidelines will be assumed by the ICCP Committee under the OECD Guidelines, which has been the central organ of the OECD projects in the field of the protection of privacy and transborder flows of personal data, as mentioned in Chapter 3 [sec. 3.1.1.1].

5.3.2 Enhancing Enforceability of the Rules by Greater "International Control"

The biennial follow-up meetings to discuss the implementation of the OECD Guidelines also put pressure on the member states to improve compliance with the rules of the OECD Guidelines.

In the OECD practice under the OECD Guidelines, at the ad hoc follow-up meetings, the names of member states which had not yet adopted the OECD Guidelines were noted in the synthesis report for each meeting. Moreover, the names of countries which had not enacted domestic data protection legislation or had not replied to the questionnaire were also reported*16.

Thus, these meetings, at which information arising from member states's domestic implementation of the OECD Guidelines was discussed on the basis of the reports prepared by the OECD Secretariat/ICCP Division, functioned as means of so-called "international control", in order to enhance the enforceability of the rules. According to the Dictionnaire de la terminologie du droit international, the term "contrôle" is defined as follows:

> Surveillance exercee en vue de vérifier la conformité d'un acte, d'une situation, de l'exercice d'un pouvoir à une règle, à un engagement ou aux exigences d'une bonne

administration, cette surveillance pouvant être qualifiée, soit en considération de l'organe ou de la collectivité qui l'exerce: contrôle international, soit en considération de son objet.[...]*17.

Furthermore, in the follow-up procedure of the 1976 Guidelines, the OECD undertook measures other than the simple collection and dissemination of information regarding the rules of the 1976 Guidelines. Those measures authorize the IIME Committee, the body designated to survey the implementation of the 1976 Guidelines, to follow up and clarify, if necessary, their rules.

Again according to the Decision C(76)117, paragraph 3 gives a mandate to the IIME Committee as follows:

> On the proposal of a Member country
> the [IIME] Committee may decide whether individual
> enterprises should be given the opportunity,
> if they so wish, to express their views concerning
> the application of [the 1976 Guidelines].
> The [IIME] Committee shall not reach conclusions on
> the conduct of individual enterprises*18.

In spite of the disclaimer in the last sentence of this paragraph, by not "interpreting", but rather "clarifying" the

content of the 1976 Guidelines, the conclusion of the IIME Committee came very close in several examples to judging the behaviour of the enterprise concerned. This quasi-judicial nature of the procedures before the IIME Committee in accordance with the mandate, which allowed solutions that might not be possible under "hard" law, can be observed for instance in the Badger case*19.

The issue in the Badger case concerned, the U.S. Badger, the parent company of a subsidiary set up as a separate corporation under Belgian law, which preferred to let the subsidiary go bankrupt rather than draw on its own funds in America to pay the separation allowance due under Belgian law to the workers of the subsidiary. Under the principle of limited legal liability, the parent company had no enforceable responsibility to cover the remaining liabilities of its Belgian subsidiary, nor did the 1976 Guidelines particularly mention any such obligation. The labor unions nevertheless claimed that multinational enterprises had a duty to meet the obligations of its subsidiary and that its failure to do so violated the spirit of the 1976 Guidelines. Based on this claim, on 23 February 1977 the Belgian delegation submitted the memorandum to the IIME Committee in accordance with paragraph 3 of the Decision, calling for an exchange views with members of the IIME Committee concerning its interpretation of the relevant paragraphs of the 1976 Guidelines. . In the

memorandum, the Belgian delegation emphasized as follows:

> It is fully understood that, in accordance with the Decision [C(76)117], the [IIME] Committee cannot reach any conclusions as to the behaviour of the enterprise in question. However, it is essential that members of the [IIME] Committee should be able to express their views on the extent to which such behaviour is compatible with the spirit or letter of certain rules of good conduct contained in [the 1976 Guidelines]*20.

It may be pointed out then that, although the point in the Badger case concerned the co-responsibility of the parent company for the obligations of its subsidiaries*21, its whole process took the form of a reconciliation of the different interpretations held by the parties concerned of the words of the the 1976 Guidelines. After fulfilling several other procedures set down by Decision C(76)117. on 31 March 1977 the IIME Committee finally concluded, in the form of expressing its clarification on the paragraphs on which the Belgian delegation asked its comments, that parent companies on a voluntary basis assumed in certain cases such financial responsibility for a subsidiary. On this basis, the Badger case was settled, with the U.S. Badger paying about twenty million Belgian francs to the Belgian subsidiary to meet compensation costs.

Therefore, from this one demonstration of international control, the Committee of Information, Computer and Communications Policy (ICCP) could also concern itself with the discussion of the same such issues and questions as arose under the OECD Guidelines, e.g. the problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgments*22. The explicit actions of fact-finding and interpretation in the individual case might not be allowed for the ICCP Committee as well as the IIME Committee, as they might bring the ICCP Committee too close to a judicial role. However, the way in which the ICCP Committee's discussion will evolve and its clarification will be expressed may indicate whether or not certain behaviour of member states should be approved by the OECD Guidelines; and through such quasi-judicial action of the ICCP Committee, the enforceability of the OECD Guidelines may be enhanced steadily.

5.4 Needs for a New Concept of "Law" in Modern International Society

5.4.1 Specific Features of Today's International Society and Its Legal Order

From the preceding discussion, it can be seen that international regulatory techniques governing TDF has been evolved, under which non-binding principles and standards are first adopted, whose acceptability and enforcement are later enhanced by feedback from case experiences and further international monitoring respectively.

Then, for more generalized consideration, the circumstances under which these techniques operate most effectively should be examined. To this end, some findings are employed concerning the features of modern international society in which legal regimes for TDF should be established. The following four points can be indicated as its specific features.

Firstly, as the international system, i.e. functional mechanism of the international society, becomes more and more integrated, international law comes to concern itself with many human activities.

Secondly, despite this, international legal order has remained less effective in comparison with domestic legal

order. The main reason is that the tripartite division of formal government institutions -- executive, legislative, and judicial -- does not readily exist at the international level. It must be recognized accordingly that in this society with horizontal legal order, the authority and effectiveness of decisions depend merely upon the voluntary compliance of legal subjects, i.e. its members.

Thirdly, although the international system has integrated swiftly, nations, the principal actors in the international politics, are still rational egoists, their preferences in international politics are based on their assessments of their own welfare, not that of others, and they seek to maximize value over a set of consistently ordered objectives. This means that centralized rule-enforcement by international organizations may remain a dream as long as the nation-states remain more "obstinate" than "obsolete"*23. Therefore, in order to ensure voluntary compliance by nations, they must agree among themselves to accept the minimum common restraint. Inevitably, they have to exchange their own arguments and claims concerning conflicting interests.

Fourthly, conflicts involving complicated issues between states, multinational enterprises and other international entities require swift, issue-specific responses. This need can be expressed by the question "Can the law keep up with the change in events?" In the field of TDF in particular, this

question must be taken into account when we seek to indicate certain conditions considered necessary for establishing effective legal regimes.

5.4.2 Responding to the Demands of Present-Day International Society: Favoured Legal Regime

Even though these specific features of the present-day international society are well understood, because every new development upsets the existing balance of interests of its participants, negotiation of a set of coercive rules is always difficult. Moreover, if participants follow the orthodox way of international law-making, namely the drafting of traditional legally-binding treaty, it would take a long enough time to miss opportunities for proper actions. This is because treaty-making, as a means of solution of present-day problems, has several major defects, a lengthy drafting process, possible delays in ratification, difficulty in making subsequent amendments[24]. To make matters worse, obsolete rules which continue to bind participants do nothing but confuse the situation.

Thus, it may be perceived that the traditional legally-binding treaty-making or decision-oriented legal regime like the domestic legal system, is not suitable for the

problems which occur in the present-day international society. Further, a favoured legal regime should be one which places more emphasis on the flexibility of its working methods to allow the fine-tuning of its existing rules to ever-changing circumstances.

5.4.3 The New Concept of "International Law" as a Process of Communication

As a response to the demands of today's international society, international regulatory techniques should take some new form other than that of traditional international law. With this new viewpoint, the experiences surrounding the OECD Guidelines with their follow-up procedures suggest certain important conditions for this new form of international "law".

The OECD Guidelines as "soft law" could overcome deadlocks in the relations between the member states that resulted from economic or political differences among them when efforts for "hard" solutions were unavailable. Moreover their follow-up procedures functioned, not only to complement the "softness" of the rules, but also to confirm and develop an acceptable legal regime over the member states. In this way, all the activities of the OECD concerning the OECD Guidelines can be regarded as the process of the exchange of different viewpoints and claims

by participants concerned.

Paying attention to this function of "claim-exchange", Prof. R. A. Falk conceives international law as a "medium of communication"*25. As a "medium of communication", law provides rhetoric, analogies, and some standards to help with the determination or whether a particular claim is reasonable*26. He describes the major contributions of law in conflict situations as follows:

> Law provides a technique for narrowing controversial claims, for communicating the precise nature of demand, for paying maximum respect to community expectations about right action, and for encouraging a rival to respond with arguments rather than weapons.*27

Therefore, through this process of "claim-exchange", or the process of "communication" among policy-makers or representatives of conflicting interests, disputes among them will be eased or prevented, a mutually beneficial compromise will be reached and a specific legal regime will be formed. For in general, the more evenly shared the regulatory interest, the smaller the need for enforcement mechanism, and the greater the prospect for effective implementation.

5.5 Concluding Remarks: the Role of International Organizations under the New Concept of "Law"

The international regulatory techniques governing TDF should be based on the premise of the dynamic process of "law" by means of "claim-exchange". Within this process, the technique of "soft law-making" can timely set minimum standards of problematic situations, such standards representing the common will of the parties interested. This technique is further accompanied by the technique of "follow-up activities" in which the following two functions are incorporated: one which improves acceptability of rules by feedback information gained from their practical application, and another which enhances enforceability of the rules by international control.

In this circular process of law, the cooperation among international parties is most likely to occur, not only when there are shared interests, but when international organizations that facilitate cooperation on behalf of those interests exist, by minimizing transaction costs, reducing uncertainty, and providing rules of thumb for government, business and labor action[28]. In particular, as previously observed in Chapter I [sec. 1.2], the field of telematics is characterized with not only the phenomenon of convergence and rapid technological changes, but also with the concern of

various branches of existing law of varied origin and separate evolution, which draw on different approaches of domestic law and which resulted in rules that were deficient and contradictory. Therefore only within the dynamic process of "communication" by means of "claim-exchange" facilitated by some international organization, the modern international society may be able to maintain the most basic level of legal order and, hopefully, international parties would be able to learn to control their inflated expectations towards the political, economic, and social benefits they wish to gain.

Footnotes to CHAPTER 5

*1 See, supra, CHAPTER 3 note 31.

*2 Hustinx, supra, CHAPTER 4 note 7 at 22.

*3 For a detailed consideration of the nature of "soft law", see R.J. Dupuy, "Droit declaratoire et droit programmatoire: de la coutume sauvage à la 'Soft Law'" (1975) S.F.D.I. [Colloque de Toulouse: L'élaboration du droit international public] at 132-148; and O. Schachter, "The Twilight Existence of Non-Binding Agreements" (1977) 71 A.J.I.L. 296.

*4 R. Baxter, "International Law in 'Her Infinite Variety'" (1980) 29 Int'l & Comp. L. Q. 549 at 565.

*5 Ibid.

*6 I. Seidl-Hohenveldern, "International Economic 'Soft Law'" (1979) 163 R.C.A.D.I. 165 at 205.

*7 The information regarding agenda of the fourth OECD ad hoc meeting of 1988 was provided during an interview in June 1988 with Mr. Muramatsu of MCA. At that meeting, recent legislative developments in Finland and the Netherlands, and modifications in existing national laws were mainly discussed. See also "OECD Reviewing Data Protection Rules" (April 1988) T.D.R. 3.

*8 R.Blanpain, The OECD Guidelines for Multinational Enterprises and Labour Relations 1976-1979 (Deventer, Netherlands: Kluwer, 1979) at 48.

*9 For the text, See Blanpain, supra, note 8 at 277-289.

*10 Seidl-Hohenveldern, supra, note 6 at 207-208.

*11 For detailed information concerning the 1979 review, see Blanpain, supra, note 8 at 237-266.

*12 For detailed information, see Blanpain, supra, note 8 at 219-228.

*13 For detailed information concerning the OECD Committee on International Investment and Multinational Enterprises, see Blanpain, supra, note 8 at 31-36.

*14 For the explanation of the new follow-up procedure refined by the 1979 review, see Blanpain, supra, note 8 at 256-263.

*15 Blanpain, supra, note 8 at 275.

*16 See, for example, OECD, "Synthesis Report on the Application of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" [OECD Doc. DSTI/ICCP/83.17] at 4. Revised version of this document [Briat, supra, CHAPTER 3 note 25] does not contain the names of countries which had not replied to the questionnaire to the synthesis report.

*17 Dictionnaire de la terminologie du droit international [publié sous le patronage de l'Union Académique Internationale] (Paris: Sirey, 1960) at 167.

*18 I. Seidl-Hohenveldern, supra, note 6 at 208.

*19 For the facts in detail, see Annex II of the Note by the Belgian Delegation, reprinted in: Blanpain, supra, note 8 at 129-130.

*20 Blanpain, supra, note 8 at 128-29 (para.2).

*21 Blanpain, supra, note 8 at 129-134.

*22 These are the problems mentioned, by some OECD member countries at the second ad hoc follow-up meeting of 1983, which have remained unsolved by the application of the OECD Guidelines. See the summary of the 1983 Synthesis Report on the application of the OECD Guidelines, contained in ANNEX 3 of this thesis.

*23 This phrase is cited from the words of Prof. S. Hoffman of Harvard University.

*24 In the best of circumstances, the drafting, signing, ratification and entry into force will require from five up to ten years. See Hondius, supra, CHAPTER 3 note 19 at 114.

*25 R.A. Falk, The Status of Law in International Society (Princeton, N.J.: Princeton University Press, 1970) at 452.

*26 R.A. Falk, Legal Order in a Violent World (Princeton, N.J.: Princeton University Press, 1968) at 68.

*27 Falk, supra, note 25 at 34. See also Falk, supra, note 26 at 67-68 and 71-74.

*28 See R.O. Keohane, After Hegemony (Princeton, N.J.. Princeton University Press, 1984) at 240.

ANNEX 1: Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the OECD, 23 September 1980)

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;

3. 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 catagories 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.

4. 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 identify 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 other 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.

ANNEX 2: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the CoE, 28 January 1981)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

N° 108

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

CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

STRASBOURG, 28.I.1981

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.

ANNEX 3: Materials concerning the Second Ad Hoc Meeting on the Follow-Up of the OECD Guidelines (10-11 March 1983). Questionnaire [OECD Doc. DSTI/ICCP/83.17] and Summary of the OECD Secretariat Synthesis Report with Regard to the Application of the OECD Guidelines [(Jan./Feb. 1984) 7 T.D.R. 4]

A N N E X I V

QUESTIONNAIRE WITH REGARD TO THE APPLICATION OF THE GUIDELINES CONCERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

The questionnaire has been divided into three sections:

- section (A) deals with the application of the principles mentioned in the Guidelines at a national level;
- section (B) deals with the application of the principles mentioned in the Guidelines at an international level;
- section (C) deals with the dissemination of the Guidelines in Member countries.

The variety of situations(1) existing in Member countries has entailed two different formulations of the questions in section (A):

- the first set of questions (I) deals with Member countries that have enacted laws directly concerning the protection of privacy;
- the second set of questions (II) deals with Member countries that have not as yet enacted laws directly concerning the protection of privacy(2).

---

(1) (a) Federal Countries are invited to state whether there is a privacy law:
* At Federal level only
* At Federal and State level
* At State level only

and to describe if there are constitutional limitations to the scope of the Federal law on privacy protection:
* the general scope of these limitations, and
* the relation between the Federal law on privacy protection and State laws on privacy protection

(b) Moreover, Federal Countries are invited, if possible, to answer the first (I) and second (II) set of questions in section (A), taking into account all the laws concerning the protection of privacy either at the Federal level or at the State level.

(2) Member countries where constitutional rules concerning the protection of privacy and/or those where sectorial or other laws only dealing with certain aspects of the protection of privacy are in force but where no laws concerning only the protection of privacy have been enacted are invited to answer this second set of questions so as to harmonise answers as much as possible.

QUESTIONNAIRE

A. The application of the principles mentioned in the Guidelines at a national level

I. Questions meant for countries where legislation directly concerning the protection of privacy is in force.

(1) Which of the eight principles of national application mentioned in the Guidelines has (or have) been the most important? Which, if any, are not applied or not fully applied?

(2) Can you specify and describe the difficulties experienced in the application of one or more of these principles?

(3) (a) Have your national laws and all legislative texts pertinent to their implementation been subject to any modifications that affect the application of these principles?

What has been the nature of these modifications?

What principles have been affected by these modifications?

- in the public sector;

- in the private sector;

(b) What use of personal records has mainly been affected by these modifications?

(c) Do these modifications result from the desire to specify or to reconcile the scope of the principles or one of the principles in relation to other legislation or preoccupations, for example, laws concerning access to administrative records (FOI) or other sectorial laws? If yes, please specify the reasons and the laws concerned.

(d) What kind of procedures have been used to arrive at these modifications?

(e) Which legal statutes or other legislative texts refer to the modifications? Could you please include a copy in your answer.

(f) Are there any other modifications foreseen for the near future? If so please specify when and to which principles they are related.

(4) Are the principles set forth in the Guidelines reflected in sectorial laws? If yes, please specify which laws and the way the principles have been taken into account.

(5) If your law foresees a system for declaration of records or a system of authorization, could you indicate by means of the following table the number of records subject to declaration or authorization?(1):

	Public Sector		Private Sector	
	from the coming into force of the law until 1980	1980/ 1982	from the coming into force of the law until 1980	1980/ 1982
Number of declarations				
Number of demands for authorization				
Number of authorizations				

(1) Federal countries are invited to indicate, if possible, the number of records subject to declaration, demand for authorization and authorization at a Federal level and the number of records subject to declaration or authorization at State level.

(6) Please describe any important court decisions or administrative decisions relevant to the protection of privacy and, if possible, send a copy.

(7) (a) Have the principles of the Guidelines been used as a basis for the establishment of systems of self-regulation, whether in the form of codes of conduct or otherwise? If so, in what cases and how?

(b) Have any firms or other entities (administrations, professional associations or other) in your country adopted systems of self-regulation, whether in the form of codes of conduct or otherwise? If so, please specify which entities and, if possible, send a copy of these codes of conduct.

(c) Please describe, if possible, the sanctions that apply in case of a breach of the code of conduct.

* * *

II. Questions meant for countries where no legislation concerning directly the protection of privacy is in force.

(1) What kind of laws could serve as a basis for the application in your country of the eight principles mentioned in the Guidelines? Please specify their nature, to which principles they relate and the substance of the relevant norms.

(2) (a) Is there a bill? If so, what stage is this at(1)?

(b) Is there a study representing an official position? If so, please provide a copy.

(c) Is there a special commission to study the introduction of a law on the protection of privacy? What stage is this at?(1)

(d) Could you specify, with the aid of the following table, the scope of the bill.

---

(1) At the date on which you answer this questionnaire.

	Yes	No
SCOPE OF THE LEGISLATION		
- Private sector and public sector (one instrument)		
- Private sector and public sector (separate instruments)		
- Public sector		
- Private sector		
- ADP and manual files		
(a) public sector		
(b) private sector		
- ADP files only		
(a) public sector		
(b) private sector		
DATA SUBJECTS		
- Physical persons and legal persons:		
(a) public sector		
(b) private sector		
- Physical persons only		
(a) public sector		
(b) private sector		
MACHINERY FOR THE ENFORCEMENT OF THE LAW(S)		
- System of declaration/registration:		
(a) public sector		
(b) private sector		
- System of authorization:		
(a) public sector		
(b) private sector		
- System of administrative appeal		
- System of judicial review		
- Other machinery		

(3) (a) What are the main provisions of the bill? In what way does the bill take into account the eight principles set forth in the Guidelines?

(b) What exceptions are specified? In particular those relevant to the eight principles set forth in the Guidelines.

(4) Please describe the machinery contemplated for the enforcement of privacy protection:

(a) Data Inspection Board or other competent institution;

(b) A system of administrative appeal; please specify the competent institutions;

(c) A system of judicial review; please specify the competent institutions;

(d) Other machinery.

(5) In what manner have the principles mentioned in the Guidelines been reflected in the bill and have they been useful in the drafting of the bill [in particular paragraph 19(c), (d), (e)]?

(6) Are the principles set forth in the Guidelines reflected in sectorial laws? If yes, please specify which laws and the way the principles have been taken into account.

(7) (a) Have the principles of the Guidelines been used as a basis for the establishment of systems of self-regulation, whether in the form of codes of conduct or otherwise? If so, in what cases and how.

(b) Have any firms or other entities (administrations, professional associations or other) in your country adopted systems of self-regulation, whether in the form of codes of conduct or otherwise? If so, please specify which entities and, if possible, send a copy of these codes of conduct.

(c) Please describe, if possible, the sanctions that apply in case of a breach of the code of conduct.

B. The application of the principles mentioned in the Guidelines at an international level

(1) (a) Do laws or bills in your country entail any rules and/or machinery to control (declaration/authorization; administrative appeal and/or judicial review) data transmission to foreign countries? If so, please specify the nature of this machinery and which data are subject to the control. Which sectors (public and/or private sector) are concerned by these rules and by this machinery?

(b) Could you give an indication as to the difficulties, if any, which have appeared with the implementation of the principles set forth in Part III of the Guidelines (paragraphs 15, 16, 17) (cases, discussions of theory or other)?

(2) Can you in view of the present situation at the international level think of cases where the exportation of personal data in the OECD area might permit the circumvention of your domestic privacy legislation? If so, which cases?

(3) (a) How do you apply the principle of paragraph 18? What kind of laws, policies and practices developed in the name of the protection of privacy create obstacles to transborder data flows of personal data that would exceed requirements for such protection?

(b) To your knowledge, have the preoccupations that figure in paragraph 20 (Part V) of the Guidelines formed the basis for information exchange on a bilateral basis? If so, under what circumstances?

(4) (a) Do you think that there is a need to improve the present situation with regard to transborder data flows and protection of privacy?

(b) To your knowledge has the application of paragraph 19 (c), (d) and (e) given rise to problems?

(c) What in your opinion, are the problems which have not yet been solved?

C. Dissemination of the Guidelines in Member countries

(1) Where applicable, have the Guidelines been translated into your official language(s)?

(2) Have either the translation or the original been circulated:

(a) in the public sector;

(b) in the private sector;

(c) to the general public;

(3) In which form have they been circulated?

(4) (a) What other means for promotion of the Guidelines have been used in your country? (workshops, medias, law and industrial conferences, etc.).

(b) What persons or bodies have been responsible for this promotion?

(5) Have the Guidelines, and more generally, the problems related to privacy protection and Transborder Flows of Personal Data in your country led to publications or press articles? If so, please supply a copy or reference.

(6) Have any firms or other entities publicly endorsed the Guidelines? If so, could you provide a list of these, and a list of the persons competent to apply the OECD Guidelines within these firms and entities.

Data Laws Create No TDF Obstacles

The OECD Secretariat, using the results of questionnaires submitted by member countries, prepared a *Synthesis Report on the Application of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (DSTI/ICCP/83.17), which was distributed at the symposium. A copy of this restricted document was made available by the US Department of State. The following is a section of the report providing a general assessment of problems which have arisen or can be contemplated as a result of the enactment of national data protection and privacy laws.

In practice, it seems that the regulation of transfers of data abroad has not constituted an obstacle to transborder data flows. No difficulties have been seen in giving effect to the fundamental principles of data protection set forth in Part III of the Guidelines. In *Austria* there have on average been two or three refusals of authorization for some 1,000 applications. Solutions to this sort of problem have been found through arrangements negotiated with the firms concerned. In *France* the most noteworthy cases have been those of Interpol, and SWIFT/Sagittaire. Problems have also arisen in connection with the transfer of social security files to foreign countries. In *Ireland* the fact that computer service industries have established themselves in the country has been a source of concern to the authorities insofar as Ireland has no legislation in this field. In the *United Kingdom* business circles have expressed concern at the commercial implications if data protection provisions are not adopted. In *Switzerland* the Interpol problem has also arisen and in the public sector data processing concerning aircraft accidents has been prohibited. There have also in Switzerland been cases of life-insurance files processed abroad. Furthermore, where files can be processed abroad it is impossible in some cases to control exportation, particularly to countries in South-East Asia.

Three member countries (the United States, Germany, Japan) take the view that it is impossible to visualize cases where the export of personal data within the OECD area would lead to circumvention of domestic legislation on privacy protection and individual liberties. *Sweden* and *Switzerland* consider that such cases may arise so long as there are still states without legislation in this field. The reply from the Canton of Vaud states that such a risk may exist due to the wide variety of national rules on the subject. Such a situation has not arisen in *Belgium* in the absence of any experience of application of legislation in force, but instances have already arisen of the collection of personal data for automated processing abroad which would be prohibited or controlled under the proposed legislation especially as regards the protection of sensitive data.

In *Norway* there is an example of a mailing list being bought from a mailing company in Norway and sold again to a West-German company which used it for illegal marketing in Norway (lottery). According to the Norwegian authorities, it is quite possible to establish personal files in foreign countries giving information on physical and legal persons resident in Norway which would not be accepted, registered or used under certain circumstances.

No laws, policies or procedures concerning the protection of privacy and individual liberties are found to create obstacles to the transborder movement of personal data over and above the standards for such protection generally accepted in member countries as a whole. Thus the control machinery in the Belgian bill is designed merely 'to guarantee the right to privacy'. Any regulation going beyond this basic legal provision would, under Belgian law, be liable to annulment *erga omnes* by the Council of State.

Bilateral exchanges of information have taken place only between Nordic countries and between Belgium and other countries. But it seems that meetings of data commissioners are the main channel for information in this field along with the OECD for the United States.

Most member countries feel that it is necessary to improve the present situation regarding transborder data flows and privacy protection, following ongoing development in this field (Sweden), the complexity of problems (United States) and the need to apply national legislation more strictly (Norway). Moreover, if such an improvement is necessary it should also be sought through international agreement (Italy).

No difficulties have emerged in the application of paragraph 19(c), (d) and (e),[1] but some problems remain unsolved according to some member countries. Two problems are the ones most often mentioned:

- the problem of liability with regard to the international communication of personal and non-personal data and the problem of principles applicable to compensation for damage suffered by data subjects due to the inaccuracy or inadequacy of personal data in a file;
- the problem of private international law:
  - determination of the forum and connecting links;
  - determination of the applicable law.

Some countries (Norway) have stressed that, for the time being, their authorities have no precise knowledge of this field. They consider that the main sectors in which major data flows are to be seen are banking and, in particular, electronic payment systems. But some time elapsed before the Norwegian data surveillance service was, for example, informed of such data flows in the case of the SWIFT system. In *Germany*, although no major problem arises, it would seem to be necessary to resolve the problem of legal persons by excluding them from the scope of privacy protection legislation.

In *conclusion*, few problems have arisen in applying the principles in the Guidlines and the large majority of member countries do not seem to have encountered difficulties in applying their national legislation to transborder data flows although the problem of the applicable law seems to be the centre of concern for some countries.■

1 Paragraph 19 states that 'Member countries should in particular endeavour to . . . (c) provide for reasonable means for individuals to exercise their rights, (d) provide for adequate sanctions and remedies in case of failure to comply with measures which implement the principles set forth in Parts II and III (e.g. principles applicable at national and international level), (e) ensure that there is no unfair discrimination against data subjects.'

ANNEX 4.

Status of Data Protection Legislation - April 1990

Country	National Legislation	OECD Guidelines	CoE Convention	
			Signed	Ratified
Australia (Rev)	L*	x		
Austria	CL	x	x	x
Belgium	L*	x	x	
Canada (Rev)	L	x		
Cyprus			x	
Denmark	L	x	x	x
Finland	L	x		
France	L	x	x	x
Germany (Rev)	L	x	x	x
Greece	(P)	x	x	
Iceland	L	x	x	
Ireland	L	x	x	x
Italy	(P)	x	x	
Japan	L*	x		
Liechtenstein	?		?	
Luxembourg	L	x	x	x
Malta	?		?	
Netherlands	CL	x	x	
New Zealand	L	x		
Norway	L	x	x	x
Portugal	CP	x	x	
Spain	C(P)	x	x	x
Sweden	CL	x	x	x
Switzerland	(P)	x		
Turkey		x	x	
UK	L	x	x	x
US	L	x		
Yugoslavia*S				

Code:

L	Law covers public/private sectors
*	Public sector only
C	Constitutional provision
P	Parliament (Congress) consideration
(P)	Draft legislation prepared
Rev	Law being revised
?	No information obtained
*S	Special status participating in the OECD

ANNEX 5: Act for Protection of Computer-Processed Personal Data held by Administrative Organs 1988 (Japan), c.95.
[(February 1989) 12 T.D.R.26 at 26ff.]

Documentation

Act for the Protection of Personal Information Processed by Computers Under the Control of Government Institutions

Chapter I – General Provisions

Section 1 – Purpose The purpose of this act is to protect the rights and interests of individuals, and to promote the proper and smooth functioning of government institutions by providing for an understanding of fundamental matters in the processing of personal information, and by considering the development of the computerized processing of personal information under the control of government institutions.

Section 2 – Definitions The definition of the following words which are used in this act shall be interpreted pursuant to each of the following: (a) A *government institution* means the following institutions: (i) government institutions which are outlined in Article 3 subsection 2 of the State Administrative Organization Act and institutions established by law under the control of the Cabinet; (ii) institutions which are specified under the special institution provided for in the State Administrative Organization Act by cabinet ordinance. (b) *Personal information* means that information recorded concerning existing individuals which can be retrieved by name, date of birth and/or any other description or number and symbol given to individuals which is included in the information. Information which cannot be retrieved by itself but can be easily related to other information and can be retrieved by such reference is also included. However, names, addresses and other information regarding directors that are included in the information of legal persons or other organizations are excluded from the definition. (c) *Computerized processing* means any input, record, editing, processing, modifying, updating, retrieval, erasure, output or other similar process which is disposed of by way of computer. But processing solely for the purpose of drawing up a composition or recording the contents of documents and drawings or other processing which is provided for by government ordinance is excluded. (d) *Personal information bank* means a collection of personal information edited systematically to perform certain office work, and that can be recorded reliably for the purpose of computerized processing by way of magnetic tape, magnetic disc or other similar medium. (e) *Processed information* means personal information recorded in the personal information file. (f) *Person in question of processed information* means that person who can be identified by any processed information which can be retrieved without referring to the name, date of birth or other description, number, mark or symbol of another individual.

Section 3 – Exceptions Personal information which was collected to prepare specified statistics provided in Section 2 of the Statistics Act and any personal information which was collected by way of statistical research reported to the director general of the Management and Coordination Agency [MCA] pursuant to Section 8(1) of the Statistics Act, and any personal information which was obtained on the requisition of a statistical report approved by the director general of the MCA pursuant to provisions of the Statistical Report Coordination Act.

Chapter II – Personal Information Processing

Section 4 – Establishment of personal information files (1) Government institutions are required to establish a personal information file (any means of collecting, recording and keeping personal information for use in their own affairs, including the processing of any personal information that is entrusted to a third party, but excluding the processing of any personal information entrusted by a third party to the institution in the course of its assigned duties). The same shall apply insofar as is necessary to perform their duties as prescribed by law which specifies particular objectives for the establishment of personal information files. (2) The scope of items recorded in the personal information file (hereinafter referred to as *recorded items in the file*) and of individuals recorded in processed information as the person concerned (hereinafter referred to as *scope of records in the file*) shall not exceed limits to the keeping of personal information necessary to attain the purposes prescribed in the preceding paragraph (hereinafter referred to as the *purpose of keeping the file*).

Section 5 – Security of personal information (1) The head of a government institution (in case of those special institutions prescribed in Section 2(a)(ii) this means that person designated by government ordinance for each institution) shall make every effort to take the necessary measures to prevent leakage, destruction or damage, and shall take whatever other steps may be required to manage personal information properly in the case of computerized processing, punching, other preparation for inputting information or in the keeping of magnetic tapes (hereinafter referred to as *computerized processing of personal information*). (2) The head of a government institution which keeps personal information files (hereinafter referred to as *keeping institutions*) shall make every effort so far as is necessary for the purpose of maintaining files to ensure that processed information corresponds with past and present facts

Section 6 – Notice in establishing personal information files (1) The head of a government institution shall give notice of the following to the director general of the MCA before the establishment of any personal information file. The same shall also apply when any change is made in the material that has been previously notified. Notice for establishing personal information files shall contain: (a) the title of the personal information file, (b) the title of the government institution that will keep the file and the name of the organization that will arrange and make use of the personal information file; (c) the purpose for keeping the file, (d) the items to be maintained and the scope of material to be included, (e) methods of collecting the information to be processed; (f) the name of any party other than the keeping institution that shall be offered continued use of any recorded information; (g) in case of a personal information file which shall appear in the personal information file register under the provision of Section 7(1) (apart from cases provided in a provisory clause of Section 13(1) and cases where the provisions of the text of Section 13(1) are not applied to all the processed information under the provisions of Section 19), the title and address of any organization which accepts application under the provisions of the text of Section 13(1); (h) in cases where part of the recorded items of the file or material provided in paragraph (e) or (f) shall not appear in the personal information file register under the provisions of Section 7(2) or in cases where the personal information file shall not appear in the personal information file register under the provisions of Section 7(3), a description to that effect; (i) in the case of a personal information file which cannot be applied for under the provisions of the text of Section 13(1) as the case shall fall within the purview of the provisory clause of Section 13(1), a statement to that effect, (j) in cases where all or part of the contents of the processed information appears in a license, permit, notice or other papers that are already issued to the person concerned, or when all or part of the contents of the processed information is made public or offered for public inspection, or when the person concerned can make a request for notice of all or part of the contents of the processed information, or when special procedures are prescribed for the processed information to which provisions of the text of Section 13(1) shall apply concerning correction, addition or deletion (hereinafter referred to as *correction, etc.*) of all or part of the contents of processed information, a statement to that effect and the title of the law or

This is an unofficial translation of the new act which was promulgated on December 16, 1988.

ordinance concerned, and (k) other matters prescribed by government ordinance. (2) The preceding subsection shall not apply to the personal information files indicated in the following paragraphs: (a) a personal information file which deals with matters concerning the security of the state, confidence of foreign affairs or other important interests of the state; (b) a personal information file which was produced or collected for the purpose of the investigation of offenses, the investigation of a breach of regulations regarding tax law or the institution and support of a public prosecution; (c) a personal information file concerning a person who is or has been a public servant of a government institution and that records only material concerning personnel records, salaries, welfare programs service and other similar material (including any personal information file concerning examinations made by government institutions); (d) a personal information file only for the use of experimental computerized processing; (e) a personal information file which records all or part of the processed information in a personal information file as set out under the provisions of the preceding subsection, and in addition the purpose for the keeping of which file and the scope and items recorded in the file are within the limits set by the notice of the given file; (f) a personal information file which records only processed information that is to be erased within one year; (g) a personal information file which is used for sending materials, moneys or other articles, or is used for necessary correspondence in the service, and that records only addresses, names and other material necessary for the sending of correspondence; (h) a personal information file which is kept by a public servant alone and used only for the purpose of performing his or her duties and only within his or her institution; (i) a personal information file which is prepared or acquired for academic purposes by a public servant on his or her own initiative and used only for the said academic purpose; (j) a personal information file in which the number of persons to be processed is under the one prescribed by government ordinances, and of which the processed information is not expected to be offered to any party other than the keeping institution; (k) a personal information file which is prescribed by government ordinances in the manner described in paragraphs (c) to (j). (3) The head of the institution keeping the files (in the case of special institutions prescribed by the government ordinances under the provisions of Section 5(1) this means the person designated by government ordinance under the provisions of Section 5(1)), shall make notice to the director general of the MCA to that effect when the institution keeping the file, of which notice has been given as prescribed for in paragraph 1, has ceased to keep the file or when the file has fallen within the purview of paragraph (j) of the preceding subsection.

Section 7 – Establishment of personal information file and public access to the file (1) The head of a government institution keeping files shall prepare a register (hereinafter referred to as the *personal information file register*) recording the material prescribed in paragraphs (a) to (g) and paragraphs (i) and (j) of Section 6(1), pursuant to the provisions of government ordinances for each personal information file which the institution concerned keeps (excluding those files enumerated in each paragraph of Section 6(2)), and give the public access to this register. (2) Notwithstanding the provisions of the preceding subsection, the head of the institution is permitted not to enter all or any part of the recorded items of the file in the register if he finds it may considerably disturb the proper functioning of those affairs for which purpose the institution keeps the file, should part of the items recorded in the file, or material enumerated in paragraph (e) or (f), enter into the personal information file register (3) Notwithstanding the provisions of subsection (1), the head of the institution keeping files is permitted not to enter any personal information file which is used for the affairs enumerated in the following paragraphs in the personal information file register if he finds it may considerably disturb the proper functioning of the affairs for which purpose the institution keeps the file: (a) affairs concerning the prevention of crime; (b) affairs concerning the international cooperation of criminal investigations; (c) affairs concerning the enforcement of custody, correction, relief or rehabilitation of criminal offenders; (d) affairs concerning the administration of emigration and immigration or the acknowledgement of displaced persons or affairs relating to the granting of visas; (e) affairs concerning the assessment and collection of a tax; and (f) affairs prescribed by government ordinances and recognized as being treated in a similar manner to the aforementioned affairs.

Section 8 – Public notice of personal information files The director general of the MCA shall make public in the official gazette at least once a year those matters enumerated in Section 6(1)(a) to (g), (i) and (j) concerning the personal information file as notified to the MCA under the provisions of Section 6(1), provided that the same does not apply to the personal information file as notified under the provisions of Section 6(3). (2) Notwithstanding the provisions of the preceding subsection, the director general of the MCA shall not make public any parts of recorded items of the files enumerated in each of the following paragraphs: (a) in the case of a personal information file parts of the recorded items of which it is decided are not to be entered in the register, according to the provisions set out in subsection (2) of the preceding section; (b) in the case of a personal information file which it is decided is not to be entered in the personal information register under the provisions of subsection (3) of the preceding section. (3) Notwithstanding the provisions of subsection (1), the director general of the MCA is permitted not to make public a personal information file on which there was no notice to modify the matters under the provisions of Section 6(1) since the last or previous publication (4) The director general of the MCA shall also make public the contents of the notification that he has received under the provisions of Section 6(3) concerning a personal information file made public under the provisions of subsection (1).

Section 9 – Restriction of the use and offer of processed information (1) Processed information shall not be used or offered for any other purpose than that for which the personal information files are kept except in cases where it is used within the institution itself or is offered to another institution in accordance with the provisions of the law (2) Notwithstanding the provisions of the preceding subsection, the head of an institution keeping a file may use or offer the processed information for purposes other than that for which the file was originally kept if he recognizes the case to fall into one of the following categories. This shall not apply to such cases where it is recognized that the rights and interests of the person concerned or of other third parties may be seriously infringed upon by the use or offering of the processed information for another purpose than that for which the file was originally kept: (a) where the person concerned agrees to such use or where the information is offered to the person concerned; (b) where the institution keeping the file uses the processed information within the institution to whatever extent is necessary to perform competently the affairs provided for by the laws, and that there are reasonable grounds for the institution to use it; (c) where processed information is offered to government institutions other than that keeping the file, local public bodies, semi-governmental corporations established directly by law or corporations established by special formalities of incorporation under special laws (hereinafter referred to as *corporations having special status*), and that those who are offered the processed information (hereinafter referred to as *the recipient*) use it only to the extent necessary to perform the affairs or business provided for by the laws, and that there are reasonable grounds for using the processed information concerned; (d) in addition to those mentioned above, in cases where processed information is offered for the preparation of statistics or for academic purposes, or in cases where it is apparent that offering the information to third parties will be to the benefit of the person concerned, or in other cases where there are special reasons for offering such processed information. (3) Those provisions of other acts of law which restrict the use or offer of processed information are not precluded from being applied by the provi-

sions of the preceding subsection (4) The head of an institution keeping a file shall restrict the inside use of information processed for any other purpose than that for which the file was originally kept to a specified department or agency if he finds a special necessity to protect the rights and interests of individuals

Section 10 – Claims to the recipient to take necessary measures (1) The head of an institution keeping a file shall impose restrictions upon the recipients of the processed information offered concerning the purposes or ways of using it, or other necessary restrictions, or shall request him to take whatever security measures are needed if he finds it necessary to offer processed information to such persons as enumerated in paragraphs (c) or (d) in subsection (2) of the preceding section under the provisions of subsection (2) of the preceding section (2) The head of the institution keeping the file shall take care not to disturb unnecessarily a person's affairs or business on the occasion of imposing restrictions or requesting necessary measures as enumerated in paragraph (c) of subsection (2) of the preceding section

Section 11 – Responsibilities of the trustee for processing The provisions of Section 5(1) shall apply correspondingly to anyone who is entrusted with the computer processing of personal information by a government institution in the performance of his or her assigned duties

Section 12 – Obligations of those in charge of the computer processing of personal information Staff or ex-staff in charge of the computer processing of personal information or any employee or ex employee engaged in assigned duties provided for in the preceding section shall not divulge or use for improper purpose any portion of personal information that has come to his or her knowledge in connection with his or her duties

Chapter III – Disclosure or Amendment of the Information Processed

Section 13 – Disclosure of information processed (1) Any person can submit a written application for disclosure (this includes cases of giving notice to a person to the effect that processed information does not exist) of processed information the subject of which is the person concerned (excluding information which is not included in the personal information file or which is not entered in the personal information registers, and any recorded items in the file which it had been decided were not to be included in the personal information file under the provisions of Section 7(2)), provided the same does not apply to any personal information file which records a person's school record or any record of the entrance examinations of schools provided for in the School Education Act, any personal information file which contains records of a person's medical examinations in any hospital, clinic or maternity clinic, or any personal information file which records trials, disposal by a public procurator, a secretary of the public procurator's office or judicial police personnel or which records material concerning the enforcement of any punishment (2) Legal representatives of minors and/or persons adjudged incompetent may apply for disclosure as set out in the preceding subsection (hereinafter referred to as *application for disclosure*) in the name of the person concerned (3) The head of an institution keeping a file shall disclose the processed information applied for in writing to the person so applying (hereinafter referred to as *the applicant*) except in cases enumerated in Section 14(1) Provided that the consent of the applicant has been obtained, the disclosure may be made by means other than in writing.

Section 14 – Cases in which personal information applied for might not be disclosed (1) The head of an institution keeping a file is permitted not to disclose all or part of the processed information applied for if he finds that the disclosure would fall under one of the following headings (a) in cases where the disclosure may disturb the proper functioning of one of the following (i) affairs enumerated in paragraphs (a) to (e) of Section 7, (ii) affairs concerning the investigation of a crime, the investigation of infringements of regulations under the provisions of the Tax Act or the institution and support of public action, (iii) affairs concerning the enforcement of an on-the spot inspection or any such other inspection under the rule of law, (iv) affairs concerning the examination of knowledge and technical expertise, review of qualifications, etc, the computation of benefits or compensation money and any other assignment or judgment corresponding to such affairs, (v) other affairs provided for by government ordinance, such as may be similar in nature to those of the preceding paragraph; (b) in cases where any disclosure of processed information may injure the proper fiduciary relations or the intimate collaboration between the institution concerned and any third party in cases where the processed information has been obtained from such a third party, (c) in cases where any disclosure may impair life, body, property or such other interests of an individual (2) The decision not to disclose all or part of the processed information under the provisions of the preceding subsection shall be made in writing and with reasons for the decision

Section 15 – Period of disclosure (1) The decision to disclose or not to disclose under the provisions of Section 13(3) (hereinafter referred to as *disclosure*) shall be made within 30 days of the time when the application for disclosure was received (2) The head of an institution keeping a file should make disclosure, etc, without undue delay from the time such disclosure becomes possible, if difficulty in performing such a task or any other reasonable grounds prevented such disclosure within the period prescribed in the preceding subsection In such a case the head of the institution keeping the file shall give notice to the applicant in writing of the reasons that the disclosure did not take place within the period prescribed above at the time of disclosure (3) The applicant may consider that it has been decided the information shall not be disclosed if disclosure, etc, is not made within the period prescribed in subsection (1) (or, in case notice has been given of intention to extend the time period before disclosure, within such a period)

Section 16 – Handling fee (1) The applicant shall pay a handling fee under the provisions of government ordinances (2) The applicant may apply for the sending of the written disclosure provided for in Section 13(3) by paying costs in addition to the handling fee provided for in the preceding subsection, except in such cases as provided for in government ordinances

Section 17 – Amendment of processed information (1) The head of the government institution shall make an investigation to whatever extent is necessary to attain the purpose for keeping the file without delay and shall give notice to the person who filed the petition of the result of the investigation in writing, excluding cases where special procedures are provided for the amendment of content, etc, of the processed information concerned in other laws and regulations, when he receives a petition in writing for amendment, etc, of the processed information by a person who had disclosure under the provisions of Section 13(1) (2) Any person who files a petition for amendment, etc, under the provisions of the preceding subsection but remains dissatisfied with the notice under the same provisions may file a petition to the head of the government institution for a review of the investigation (3) The provisions of subsection (1) shall apply correspondingly to any case in which a petition is filed under the provisions of the preceding subsection

Section 18 Commitment to government ordinance Necessary material concerning the items mentioned in writing under the provisions of Section 13(1), Section 14(2), Section 15(2) and subsection (1) of the preceding section, any necessary papers for the application for disclosure by a legal representative under the provisions of Section 13(2), any procedure necessary to identify the ap

plicant to be the subject of any processed information, and any other material necessary for the application for disclosure, method of disclosure and amendment of processed information shall be provided for by government ordinances

Section 19 – Relation to other laws The provision of the text of Section 13(1) shall not apply to all or part of the processed information concerned when all or part of the contents of such processed information is mentioned in any license, permit, notice or other such papers as have already been delivered to the person concerned, when all or part of the processed information has been made public or offered for public perusal, or when the person concerned in the processed information can apply to make all or part of the processed information known to him

Chapter IV – Miscellaneous Rules

Section 20 – Complaint handling The head of the government institution shall make every effort in the fast and proper handling of complaints concerning the use, offer or disclosure of processed information and concerning petitions for the amendment of the processed information and any other complaints concerning the handling of the processed information

Section 21 – Request for submission of materials and explanations The director general of the MCA may make a request to the head of a government institution for the submission of materials and explanations, when he finds it necessary to do so, concerning the operating practices involved in the computer processing of personal information at that government institution.

Section 22 – Statement of the director general The director general of the MCA may advance an opinion to the prime minister or the head of any government institution concerning the handling of personal information processed by computers kept by a government institution when he finds it necessary in order to attain the purposes of this act

Section 23 – Delegation of power or matters The head of an institution keeping a file may delegate power or matters provided for in Section 9(2), Section 10(1), Section 13, Section 14, Section 15(2) and Section 17(1) to staff of the institution concerned by provision of government ordinance.

Section 24 – Government ordinances In addition to the provisions of this act material necessary for the implementation of the act shall be provided for by government ordinance.

Section 25 – Penalty Any person who obtains disclosure under the provisions of Section 13(3) through false representation or other unjust means shall be liable to a correctional fine of not more than JPY100,000.

Section 26 – Responsibility of local public body Any local public body shall take every necessary measure to secure the proper handling of personal information, taking into consideration the national measures under the rule of the act, and shall take steps to implement it when engaged in the computerized processing of personal information

Section 27 – Responsibility of corporations having special status Corporations having special status shall take every necessary measure to secure the proper handling of personal information, taking into consideration the national measures under the rule of the act, when engaged in the computerized processing of personal information

Supplementary Provisions

Date of enforcement This act shall be enforced on the date fixed by government ordinance within one year of its promulgation However, the provisions of Chapter III and Section 23 (excluding the provisions concerning Section 9(2) and Section 10(1)) shall be enforced on the date fixed by government ordinance within two years of the promulgation of the act.■

ANNEX 6: Guidelines on the Protection of Personal Data for Financial Institutions (the Center for Financial Industry Information System: FISC (Tokyo, JAPAN), March 1987)

I. Nature of the Guidelines

1. Basic points of view

(1) In recent years, rapid increases in the various applications of computers, coupled with the progress in communications technology, which have made possible the processing of a large amount of data within seconds, have contributed greatly to the advancement of the information society.

In this context, however, there has been mounting concern about the potential dissemination and process of personal data without being noticed by the data subject, or in other words, an infringent mf privacy. Accordingly, various opinions requiring to study how to cope with the situation have been expressed heretofore.

(2) It has become necessary to harmonize the handling and protection of personal data among countries because numerous data processing systems and communication networks carrying various data across national frontiers have been installed. The United States and the leading countries of Europe have already taken some legislative or other measures on the protection of personal data in accordance with the Recommendation by the Council of the OECD(*1) (hereinafter referred to as "the OECD Guidelines") and the Convention of the Council of Europe.(*2) Thus Japan will also be urged to deal with the protection of personal data appropriately.

(3) Taking the above into consideration, in March 1987 the FISC has made up the guidelines on the protection of personal data for financial institutions(#) based on the free will of financial institutions.

2. Effect of the Guidelines

The FISC was incorporated in 1984 as a nonprofit organization under the imprimatur of the Ministry of Finance. It has been doing various activities such as making and publishing guidelines, making researches, and others with emphasis on computer systems and networks installed or connected to financial institutions for its members including financial institutions, computer manufacturers and

communication service providers.

The Guidelines were drawn up after deliberations at the Expert Committee on Personal Data Protection of the FISC, which consists of experts representing academia and members of the FISC such as banking institutions, insurance companies, securities companies and credit card companies.

Financial institutions are indicating their intention to handle personal data appropriately in accordance with these Guidelines. In other words financial institutions are responding to the OECD Guidelines.

(#) "financial institutions" in these guidelines covers insurance companies securities companies and credit card companies as well as financial institutions in the strict sense.

II. Guidelines on the Protection of Personal Data for Financial Institutions

To ensure the protection of personal data, financial institutions should act in accordance with the following guidelines with regard to automatic processing of personal data. Hereafter "personal data" refers to any information relating to an identified or identifiable individual ("data subject").

1. Collection of Personal Data

(1) The collection of personal data should be limited to the extent necessary to conduct business as specified under laws and regulations concerning financial institutions.

(2) Personal data should be obtained by lawful and fair means.

(3) In collecting personal data from a third party, financial institutions should strive to avoid imparting unwarranted harm to any interests of the data subject worthy of protection.

[Comments]

A) This section corresponds to the "Collection Limitation Principle" and the "Purpose Specification Principle" of the OECD Guidelines.

B) Personal data should be collected for specified purposes and only to the extent necessary for the fulfillment of those purposes. The business of financial institutions in Japan is specified and its scope is strictly limited by such laws and regulations as the Banking Law, the Securities and Exchange Law, the Insurance Business Law, etc. Therefore, the expression "to the extent necessary to conduct business" will satisfy the principles mentioned above in the case of financial institutions.

C) It is necessary for financial institutions to handle personal data fairly and lawfully. This requirement should be taken into full account especially in collecting personal data.

D) No problems arise in reference to personal data protection, when personal data are collected directly from the data subject, as the data subject is aware of the purpose of collection and discloses the personal data at his own discretion. However, problems may arise when the personal data are collected from a third party, as the data subject is usually unaware of the data collection. For this reason, in collecting personal data from a third party, financial institutions should make strong efforts to avoid imparting unwarranted harm to any personal interests of the data subject worthy of protection.

2. Use and Disclosure of Personal Data

(1) Use of personal data in financial institutions should, in principle, be limited to the confines of business specified by laws and regulations concerning financial institutions.

(2) Disclosure of personal data to third parties should be limited to those cases where:

a) the disclosure is within the confines of business specified by laws and regulations concerning financial institutions, or is requested to ensure justifiable interests of the data recipients, and is not likely to damage justifiable interests of the data subject worthy of protection; or

b) the data subject consents to disclose the personal data to third parties; or

c) the requests for the disclosure are made for the public interest, including requests under laws and regulations.

[Comments]

A) This section corresponds to the "Use Limitation Principle" of the OECD Guidelines.

B) As mentioned in the previous section on "Collection of Personal Data", the business of financial institutions is specified and the scope of business is strictly limited. Therefore, financial institutions which use personal data only within the

confines of their business are considered to meet the purport of the above-mentioned principles.

C) Financial institutions often handle sensitive personal data such as credit information, medical information, etc. The data transacted with financial institutions are generally expected to be handled with deliberation for the individual's sake. Therefore, financial institutions should make special efforts to protect the personal data when they disclose such personal data to third parties. Moreover personal data should not be disclosed to third parties except in cases described below.

a) Financial institutions are able to disclose personal data to third parties when the disclosure is within the confines of business and is not likely to damage justifiable interests of the data subject worthy of protection. They are also able to disclose personal data to third parties when the disclosure ensures socially justifiable interests of data recipients, for instance, minimizing business risks, and is not likely to harm justifiable interests of the data subject worthy of protection.

However, in light of the public role of financial institutions and customers' reliance on them, it is requested that the disclosure should be made with deliberation, for instance, only when it is expected that the protection of personal data concerned is certainly assured after the disclosure.

b) When the data subject consents to the disclosure, financial institutions are entitled to disclose personal data to third parties. The consent of the data subject is required in advance for the disclosure of personal credit information to a credit bureau, mainly because of the greater possibility of the data being widely used in the financial system.

c) (2)-c) mentioned above refers to cases where the request for disclosure is made to financial institutions under the provisions of laws and regulations authorizing a search warrant, inspections, etc and other cases where authorities concerned determine that the disclosure is necessary for public interests.

3. Proper Management of Personal Data

(1)	Personal data should be kept accurate to the extent necessary for their proposed use. The period of time that personal data is to be stored on file should, in principle, be specified.
(2)	Personal data should be protected by reasonable security safeguards against such risks as unauthorized access, loss, destruction, modification, leakage, etc.
(3)	In the event that the processing of personal data is entrusted to a third party, terms should be provided in the contract with regard to maintenance and management of data including keeping confidentiality.

[Comments]

A) This section corresponds to the "Data Quality Principle" and the "Security Safeguards Principle" of the OECD Guidelines.

B) The use of inaccurate data concerning any individual is likely to have undesirable effects on the individual as a result of misrepresentation. Personal data should be kept accurate to avoid such effects. Data, even if accurate at the time of input, could become outdated at a later date. Therefore, personal data should be kept up-to-date and accurate. There are, however, practical limits to keeping all personal data accurate and up-to-date. Data revision might not always be necessary, depending on the frequency of business transactions and use, etc. Accordingly, financial institutions should endeavor to keep personal data accurate and up-to-date to the extent necessary for the intented use.

C) It is not only desirable to specify the period of time for which data are stored on file to keep the data accurate and up-to-date, but is also effective for personal data protection because if the data are deleted at the expiration period, the possibility of undesirable effects on the data subject can be reduced to that extent.

It is difficult to specify uniformly how long data should be retained on file because of differences of business characeristics, data systems and others.

Therefore, it is reasonable to leave this decision to the individual financial institutions.

D) In connection with keeping personal data accurate, when inaccurate data are found and corrected, it is desirable to the data recipients to be notified the correction, provided they can be reached.

E) Security measures to personal data are included in the computer system security. Measures necessary for the protection of data are also given in detail in "Computer Systems Security Guidelines for Financial Institutions"(*3) made by the FISC in December 1985. These measures are established by the financial institutions themselves as the guidelines for personal data protection.

F) When the processing of personal data is entrusted to a third party by financial institutions, maintenance and management of data measures should be taken in order to prevent the third party from leaking data. In the event that the personal data processing is carried out entirely by the third party from imput to maintenance and storage, it will be necessary to make an agreement of establishing comprehensive security safeguards of data on the part of the third party.

4. Individual Participation

(1) Requests by the data subject backed by identification to gain access to his personal data should be accepted as far as possible, except in cases where it is considered inappropriate to inform the subject of the content in light of customary practices etc.
(2) Requests to correct errors in personal data, should be accepted without delay.

[Comments]

A) This section corresponds to the "Openness Principle" and the "Individual Participation Principle" of the OECD Guidelines.

B) Financial Institutions should strive to keep data accurate and up-to-date. In addition it is helpful for the data subject to have a means for checking accuracy of

the data personally when there are doubts about the data for some reason.

Incidentally, financial institutions provide their customers with such data, on request, as deposit and loan balances and credit and debit transactions. Few requests have been made for other data. However, upon request and proper identification, financial institutions are prepared to furnish individuals with data as far as possible.

C) As to data disclosure requested by the data subject, it is inappropriate to disclose all the personal data relating to himself that financial institutions hold.

In light of the privacy of the general public and customary practices, it is reasonable to withhold certain data such as individual evaluation and medical history, which are not supposed to be disclosed to the data subject. In addition, replying uniformly to all data requests would interrupt operations at financial institutions. Unspecified requests, requests for a means of collecting data and the records of data use and disclosure, etc. are considered unacceptable.

D) In the event that data are incorrect and a request for correction or deletion is made, it should be accepted since it is difficult to specify when data should be corrected or deleted. It is reasonable to say that the correction should be made without delay.

When data are disclosed to a third party and the data subject makes a request to furnish a notification of the correction to the party which has received incorrect data, the notification should be made without delay, provided that the party can be reached.

E) Financial institutions may impose a reasonable charge on a person who requests data disclosure unless the request is to amend inaccurate data.

It is expected that an appropriate study should be made on charges for disclosure to the data subject at individual financial institutions.

NOTES

(*1) Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted on September 23, 1980.

(*2) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted on September 17, 1980.

(*3) Computer System Security Guidelines for Financial Institutions consist of 228 items in all which are grouped under three board categories namely physical security, hardware/software security and procedural security.

The main objectives of them are to prevent system failures caused by natural or other disasters, hardware or software malfunctions and illegal operations.

FISC

The Center for Financial Industry Information Systems

Background

Aggressive implementation of Electronic Funds Transfer Services has been providing much better services for bank's customers, and improving the efficiency of banks in the last several years in Japan.

In addition, new issues are pointed out to be discussed in advance, in order to avoid the expected confusion coming from the changing financial services.

The Center for Financial Industry Information System (FISC), organized in November, 1984, by about 1000 financial institutions, associations, computer makers and others, is established to research the new issues on EFT services, and examine necessary measures for the appropriate approach to the sophisticated network society in the future.

Role and Activities

1. Research and study of problems and issues on the electronic financial information serfices.
2. Investigation of the financial information systems security.
3. Development and promotion of the financial information systems security and the personal data protection.
4. Development and promotion of EDP audit.
5. Investigation of the feasibility of the co-operative financial services.
6. Introduction of the software products for electronic financial services.
7. Organizing the conferences and the symposiums regarding the electronic financial services.
8. Publishing journals and papers.
9. Other programs on electronic financial services.

16th Floor ARK Mori Building
12-32, 1 Chome, Akasaka, Minato-ku, Tokyo 107
Japan
Phone: 81-3-505-7711
Fax: 81-3-589-5559

BIBLIOGRAPHY

to

LEGAL ASPECTS OF TRANSBORDER DATA FLOWS AND PROTECTION OF PRIVACY: Contemporary Developments in Establishing Legal Regimes over a Rapidly Emerging Field of Telematics

by

Ikuko OTA

INSTITUTE OF CCMPARATEIVE LAW
McGILL University
Montreal, Quebec
CANADA

September 1990

BIBLIOGRAPHY

AKEHURST, M. "The Hierarchy of the Sources of International Law." B.Y.I.L. 47 (1974-75): 1-53.

ALEXANDROWICZ, C.H. The law of Global Communication. New York: Columbia University Press, 1977.

AMERICAN BAR ASSOCIATION, Science and Technology Section. Toward a Law of Global Communications Networks. edited Branscomb, A.W. New York and London: Longman, 1986.

AMORY, B.E. "Proposed EEC Directive on Legal Protection of Semiconductor Products." Computer Law Practice (May/June 1986): 161.

BAADE, H.W. "The Legal Effects of Codes of Conduct for Multinational Enterprises." German Yearbook of International Law 22 (1979): 11-52.

BECKER, R.K.A. "Transborder Data Flows : Personal Data - Recommendations of the Organization for Economic Cooperation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C(80)58 (Oct. 1, 1980)." Harvard International Law Journal 22 (1981): 241-47.

BLANPAIN, R. The OECD Guidelines for Multinational Enterprises and Labour Relations 1976-1979. Deventer, Boston and London: Kluwer, 1979.

BOTHE, M. "Legal and Non-Legal Norms." The Netherlands Year Book of International law 9 (1980): 65-96.

BRANSCOMB, A.W. "Global Governance of Global Networks: A survey of Transborder Data Flow in transition" Vanderbilt L.Rev. 36 (1983): 985-1043.

---------- "Who Owns Information?" T.D.R. (January 1986): 9-11.

BROWNLIE, I. "Legal Status of Natural Resources in International Law: Some aspects."

Recueil des Cours I (1979): 249-317.

BURKERT, H. "Institutions of Data Protection--an Attempt at a Functional Explanation of European National Data Protection Laws." Computer L.J. 3 (1982): 170-88

CANADIAN COUNCIL ON INTERNATIONAL LAW International Regulation and Deregulation: Emerging tronds in the role of international institutions. Proceedings of the 14th annual conference of the C.C.I.L. in Ottawa, Canada, October 17-19, 1985.

COLE, P.E. "New Challengers to the U.S. Multinational Cooperation in the European Economic Community: Data protection laws." New York University Journal of International Law and Politics 17 (1985): 893-947.

COOPER, D.M. "Transborder Data Flow and The Protection of Privacy: The harmonization of data protection law." The Flecher Forum (Summer 1984): 335-52.

COPLIN, W.D. The Functions of International Law: An introduction to the role of international law in the contemporary world. Chicago: Ranel McNally, 1966.

Council of Europe. Information Bulletin on Legal Activities: Within the Council of Europe and in member states 14 (1983): 15-17,
21 (1985): 15-16.

CULLEN, A. "Electronic Information Services--an Emerging Market Opportunity?" Telecom. Pol'y (December 1986): 299-312.

DAVIDOW, J. & CHILES, L. "The United States and the Issue of the Binding or Voluntary Nature of International Codes of Conduct Regarding Restrictive Business Practices." A.J.I.L. 72 (1978).

DESJARDINS-SICILIANO, Y. Recueil de Textes et Arrêts Préparé Pour les Etudiants du Cours Droit de l'Informatique. Université de Montréal, Faculté de Droit (1986).

DUPUY, R.J. "Droit Déclaratoire et Droit Programmatoire: De la coutume sauvage à la 'soft law'." In

L'élaboratien du droit international public, by Société francaise pour le droit intrenational Colloque de Toulouse (1975): 132-48.

DURKA, W.J. "Legal Issues of Transborder Data Transmission." AM. SOC'Y INT'L L. PROC. 74 (1980): 175-78.

EARLY, T.L. "Recent Developments in Data Production in the Council of Europe." Computer L.& Prac. (November/December 1986): 68-69.

EGER, J.M. "Emerging Restrictions on Transborder Data Flows: Privacy protection or non-tariff trade." Law and Policy in International Business 10 (1978): 1055-103.

----------. "The Global Phenomenon of Teleinformatics: An introduction." Cornell Int'l L.J. 14 (1981): 203-36.

FALK, R.A. "The Regulation of International Conflict by Means of Law." In Legal Order in a Violent World, 39-79. Princeton: Princeton University Press, 1968.

----------. The Status of Law in International Society. Princeton: Princeton University Press, 1970.

----------. "The Role of Law in World Society: Present crisis and future prospects." In Reisman, W. and Weston, B., ed., Toward World Order and Human Dignity. Free Press, 1976.

FELDMAN, M.B.& GARCIA, D.R. "National Regulation of Transborder Data Flows" North Carolina Journal of International Law and Commercial Regulations 1, (1982).

FISHMAN, W.L. "Introduction to Transborder Data Flows." Stan. J. Int'l L. 16 (1980): 1-26.

----------. "Some Policy and Legal Issues in Transborder Data Flow." Am. Soc'y Int'l L. Proc. 74 (1980): 179-87.

FROSINI, V. "The European Convention on Data Protection." Computer L.& Prac. (January/February 1987): 84-90.

GOLD, J. "Strengthing the Soft International Law of Exchange Arrangements." A.J.I.L. 77 (1983): 443-489.

GRANT, P.S., Chairman. Freedom of Information and Individual Privacy. An international symposium co-sponsored by
The Law Society of Upper Canada, Toronto, CANADA
The International Freedom of Information Commission, London, U.K.
The Canadian Bar Association, Ottawa, CANADA,
held in Toronto 26-27 September 1980.

GRAY, S.J. Information Disclosure and the Multinational Cooperation. WILEY/IRM Series on Multinationals. John Wiley & Sons, 1984.

HAMMOND, R.G. "The Misappropriation of Commercial Information in the Computer age." The Canadian Bar Review 64 (1986): 342-73.

HERTY, D. "On Making Data Protection Effective." T.D.R. (April 1986): 15-16.

HOFFMANN, S. "International Organization and the International System", International Organization 24 (1970): 389-413.

HONDIUS, F. "Data Law in Europe." Stan. J. Int'l L. 16 (1980): 87-111.

HORGAN, S.M. "Foreign Data: Is it safe in United States data bank?" California Western International Law Journal 16 (1986): 346-72.

International Chamber of Commerce, Special Joint Committee on Uniform Rules for Communication Agreements. "Draft Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission(UNCID)." Computer L.& Prac. (January/February 1987): 105-9.

JENNINGS, R.Y. "Recent Developments in the International Law Communication: Its relation to the source of internation law." Internaional and Comparative Law Quarterly 13 (1964): 885-97.

KEOHANE, R.O. After Hegemony.

Princeton: Princeton University Press, 1984.

KIMBEL, D. "Policy Research for Information Activities--The OECD Programme on Information, Computers and Communications Policy." Telecom. Pol'y (December 1977): 367-73.

KIRBY, M.D. "Transborder Data Flows and the 'Basic Rules' of Data Privacy." Stan.J. Int'l L. 16 (1980): 27-66.

----------. "The Morning Star of Informatics Law and the Need for a Greater Sense of Urgency." Government Publications Review 12 (1985): 203-14.

----------. "The Ten Information Commendments." T.D.R. (June 1986): 19-22.

KLINE, J.M. International Codes and Multinational Business. Westport, Conneticut: Quorum Books, 1985.

MANDELL, S.L. Computers, Data Processing, and the Law. St.Paul, New York: West Publishing Company, 1983.

MATTE, N.M. & JAKHU, R.S. Canadian Law of Communications. A report submitted to Max-Planck-Institute, Hamburg, West Germany, 1985.

McDOUGAL, LASSWELL & REISMAN. "The Intelligence Function and World Public Order." Temple Law Quarterly 46 (1973): 365-

McWHINNY. E. The World Court and the Contemporary International Law-Making Process. Sijthoff & Noordhoff Alphen aan den Rijn, the Neitherlands: Sijthoff & Noordhoff, 1979.

----------. United Nations Law Making. New York: Holms & Meier Publishers, 1984.

NOVOTNY, E.J. "Transborder Data Flows and International Law: A policy-oriented framework of inquiry." Stan.J. Int'l L. 16 (1980): 142-80.

----------. "Transborder Data Flow Regulation: Technical issues of legal concern." Computer L.J. 3 (1982): 105-24.

OECD. Activities of OECD in 1981. Paris: OECD, 1982.
in 1982. (same as above), 1983.
in 1983. (same as above), 1984.
in 1984. (same as above), 1985.

----. Transborder Data Flows and the Protection of Privacy. ICCP Series No. 1. Paris: OECD, 1979.

----. Policy Implications of Data Network Developments in the OECD Area. ICCP Series No. 3. Paris: OECD, 1980.

----. Handbook of Information, Computer and Communications Activities of Major International Organizations. ICCP Series No. 4. Paris: OECD, 1980.

----. An Exploration of Legal Issues in Information and Communication Technologies. ICCP Series No. 8. Paris: OECD, 1984.

----. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 1981.

----. OECD Observer. (1962-)

ONUF, N. G., ed. Law-Making in the Global Community. Durham, North Carolina: Carolina Academic Press, 1982.

O'REILLY, J. "Regaining a Confidence: Protection of business confidential data through the reform of the Freedom of Information Act." Ad. L. Rev. 34 (1982): 263-313.

PIPE, G. R. "Searching for Appropriate TDF Regulation." T. D. R. Vol. VII No. 1 (1984): 1-10.

PLAINE, . . "The OECD Guideline for Multinational Enterprises." Int'l Lawyer 11 (1977): 339-46.

PLOMAN, E. W. "Transborder Data Flows: The international legal framework." Computer L. J. 3 (1982): 551-62.

POOL, I. & SOLOMON, R. J. "The Regulation of Transborder Data Flows." Telecom. Pol'y (September 1979): 176-91.

RAMSEY, T. J. "Europe Responds to the challenge of the New Information Tecnologies: A teleinformatics

strategy for the 1980's." Cornell Int'l L.J. 14 (1981): 237-86.

REISMAN, W.M. "International Lawmaking: A process of communication." (The Harold D. Lasswell memorial lecture) Am. Soc'y Int'l Proc. 75 (1981): 101-20.

RELYEA, H.C. "Business, Trade Secrets, and Information Access Policy Developments in Other Countries: An overview." Ad. L. Rev. 34 (1982): 315-71.

ROBERTSON, A.H. The Council of Europe: Its structure, functions and achievements. London: Stevens, 1961.

ROSTOKER, M.D. & RINES, R.H. Computer Jurisprudence. New York: Oceana Publications, Inc., 1986.

RUBIN, S.J. "The International Legal Effects of Unilateral Declarations." A.J.I.L. 71 (1977): 1-30.

----------. "International Code of Conduct on the Transfer of Technology." A.J.I.L. 73 (1979): 319-20.

RUSSELL, H.S. "The Helsinki Declaration: Brobdingnag or Lilliput?" A.J.I.L. 70 (1976):

SANDERS, P. "Implementing International Codes of Conduct for Multinational Enterprises." American Journal of Comparative Law 30 (1982): 241-54.

SAUVANT, K.P. "Trade in Data Service: The international context." Telecom. Pol'y (December 1986): 282-98.

SCHACHTER, O. "The Twilight Existence of Non-binding International Agreements." A.J.I.L. 71 (1977): 296-304.

----------. "Towards a Theory of International Obligation." In SCHWEBEL, ed., The Effectiveness of International Decisions, 9-31. Leyden: A.W. SIJTHOFF, 1971.

SCHWARTZ, R. "Are the OECD and UNCTAD Codes Legally Binding?" Int'l Lawyer 11 (1977): 529-36.

SIDDLE, J. "The Role of the Council of Europe in the Legal Field." European Law Review 2 (1977): 335-47.

SKUBISZEWSKI, K. "Enactment of Law by International Organizations." B.Y.I.L. 41 (1965-1966): 198-274.

STEINER, H.J.& VAGTS, P.F. Transnational Legal Problem--Materials and Text. 3rd ed. Mineola, N.Y.: Foundation Press Inc., 1986.

Symposium on Transborder Data Flows. Transborder Data Flows: Proceedings of an OECD conference held [London, England] December 1983. North-Holland, 1985.

TURN, R. "Privacy Protection and Security in Transnational Data Processing Systems." Stan.J.Int'l L. 16 (1980): 67-86.

United Nations Centre on Transnational Corporations Transnational Corporations and Transborder Data Flows: A technical paper. [United Nations ST/CTC/23, 1982] New york: United Nations, 1982.

UN Legistlative Series. Review of Multinational Treaty-Making Process. (ST/LEG/SER.B/21, 1985).

VIRALLY, M. "La deuxième décennie des Nations Unies pour le dévelopment, Essai d'interpretation para-juridique." Annuaire francais de droit international 16 (1970): 9-33.

WACKS, R. The Protection of Privacy. Modern Legal Studies. London: Sweet & Maxwell, 1980.

WESTIN, A.F. Privacy and Freedom. London: Mandell, 1984.

WIEL, P. "Towards Relative Normativity in International Law?" A.J.I.L. 77 (1983): 413-42.

YARN, D. "The Development of Canadian Law on TBDF." Georgia Journal of International and Comparative Law 13 (1983): 825-55.

YUROW, J.H. (ed.) Issues in International Telecommunications Policy: A sourcebook. The George Washington University, Center For Telecommunications Studies, 1983.

ZIMMERMAN, J.A. "Transborder Data Flows: Problems with the Council of Europe convention, or protecting states from protectionism." Northwestern Journal Law & Business 4 (1982): 601-25.